National Security
Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CAMPUS WIRELESS LOCAL AREA NETWORK CAPABILITY PACKAGE

This Commercial Solutions for Classified (CSfC) Capability Package (CP) describes how to protect classified data using wireless devices to access sensitive data and enterprise services when connecting to Government-Owned Wi-Fi networks using Wi-Fi Protected Access (WPA) 2 as the outer layer of protection and IPsec as the inner layer of protection.

Version 1.8
September 17, 2015

Campus WLAN Capability Package

CHANGE HISTORY

Title	Version	Date	Change Description
Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package	0.9	December 14, 2012	• Initial release of CSfC Campus IEEE 802.11 Wireless Local Area Network (WLAN) guidance.
Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package	1.0	August 20, 2013	• Official release of CSfC Campus WLAN guidance. • Revised content to be consistent with VPN CP version 2.0. • Removed compound requirements for improved testability. • Merged sections to reduce duplicate requirements.
Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package	1.1	March 4, 2014	• Corrected minor errors • Removed redundant requirements • Added Solution testing section • Added Appendix F to state summary of changes in requirements between the versions
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	1.8	September 17, 2015	• Initial release of CSfC Campus WLAN guidance for use of a Shared Outer WPA2 layer and single Gray Network with networks of multiple security levels. • Improvements of Continuous Monitoring and revised content to be consistent with VPN CP version 3.2 and MA CP version 1.1. • Added new Cryptography standards in accordance with CNSSP 15. • Added Gray Firewall • Added Continuous Monitoring Requirements • Updated requirement WLAN-PS-10

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages (CP) to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CPs are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.

IAD is delivering a generic CSfC Campus Wireless Local Area Network (WLAN) CP to meet the demand for commercial End User Devices (i.e., tablets, smartphones, and laptop computers) to access secure enterprise services over a campus wireless network. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. Campus WLAN CP Version 1.8 enables customers to implement layered encryption between a Red Network and End User Devices (EUDs). This CP takes lessons learned from 3 proof-of-concept demonstrations. These demonstrations included a layered use of COTS products for the protection of classified information. The CSfC Campus WLAN CP Version 1.8 supersedes the Campus IEEE 802.11 WLAN CP Version 1.1 dated 04 March 2014.

2 PURPOSE OF THIS DOCUMENT

This CP provides reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List for their Campus WLAN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 11, customers must ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected architecture. Throughout this document, requirements imposed on the Campus WLAN solution, to ensure proper implementation, are identified by a label consisting of the prefix "WLAN," a two-letter category, and a sequence number (e.g., WLAN-KM-11). To successfully implement a solution based on this CP, all Threshold requirements, or the corresponding Objective requirements, must be implemented, as described in Sections 10-1.

Customers who want to use this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3 USE OF THIS DOCUMENT

This document may not be used for a CSfC solution without formally obtaining support from NSA for the effort prior to presenting a solution to the implementing organization's Authorizing Official (AO). United States Government entities interested in presenting solutions to their AOs in accordance with this guidance must first obtain NSA support by submitting a request for CP application support to their NSA/IAD Client Advocate. In the future, however, customers and their solution providers will be able to use a later version of this guidance to implement solutions without such NSA/IAD involvement. Until

that time, customers and solution providers may still register solutions designed according to Version 1.1 of the Campus WLAN CP, dated 4 March 2014; see Section 3 of that document for details.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the Campus WLAN CP maintenance team at Wi-Fi@nsa.gov

CNSS Policy No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems (NSS)*, is in the process of being updated to reflect the recently published CNSS Advisory Memorandum (AM) Information Assurance (IA) 02-15. CNSS AM IA 02-15 expands on the guidance contained in CNSS Policy No. 15 and identifies additional public algorithms to protect information within NSS. Specifically, the following algorithms will be required to protect all NSS up to Top Secret:

- AES 256 (confidentiality)
- RSA 3072 or ECDSA P-384 (digital signature and authentication)
- RSA 3072, DH 3072 or ECDH P-384 (key exchange)
- SHA-384 (hashing and integrity)

Vendors are strongly encouraged to meet the objective algorithm requirements for WPA2 and EAP-TLS as soon as possible to comply with AM-02-15 and the forthcoming update to CNSS Policy No. 15.

Campus WLAN CP solutions shall also comply with Committee on National Security System (CNSS) policies and instructions. Any conflicts identified between this CP and NSS or local policy should be provided to the Campus WLAN CP Maintenance team.

The following Legal Disclaimer relates to the use of this CP:

This CP is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The user of this CP agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DESCRIPTION OF THE CAMPUS WLAN SOLUTION

The Solution described within this CP is supported by the use of wireless devices to access sensitive data and enterprise services while minimizing the risk when connecting to existing Government enterprise networks. Government-managed campus-area wireless networks provide controlled connectivity between mobile users and the broader Government enterprise. The term "Campus" is used in this document to refer to any area which is physically protected to the highest classification level of the red network where multiple enclaves are supported. This physical area includes secure facilities and tactical environments when the physical controls are deemed appropriate by the Authorizing Official.

The Campus WLAN solution uses two layers of cryptography, Internet Protocol Security (IPsec) using AES 256 and WPA2 using AES 128, to protect the confidentiality and integrity of the data as it transits the untrusted network. The two layers protecting a data flow are generated by the Virtual Private Network (VPN) Client and WLAN Client running on an EUD. Figure 1 depicts at a high level the Campus WLAN solution within the context of the basic segments of the Campus WLAN architecture. Implementing a WLAN solution that uses two layers of IPsec encryption, a customer has the option of complying and registering with the Mobile Access CP version 1.1 instead of this CP.

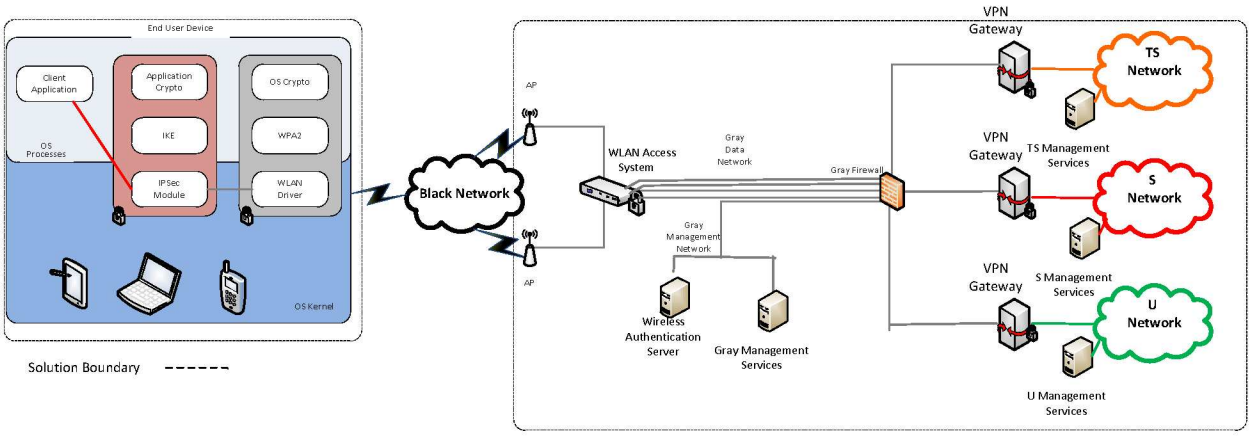

Figure 1. Overview of Campus WLAN CP

Campus WLAN solutions are composed, layered, and built using products from the CSfC Components List. Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the vendors to encourage them to sign a Memorandum of Agreement (MOA) with NSA and start the National Information Assurance Partnership (NIAP) evaluation process, which will enable them to be listed on the CSfC Components List. Products listed on the CSfC Components List are

not guaranteed to be interoperable with all other products on the Components List. Customers and Integrators should perform interoperability testing to ensure the components selected for their Campus WLAN Solution are interoperable. Customers needing assistance obtaining vendor POC information should email csfc_components@nsa.gov.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their integrators are advised that modifying a NIAP-evaluated component in a CSfC solution may invalidate its certification and trigger a revalidation process. To avoid delays, customers or integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (see http://www.niap-ccves.org/Documents_and_Guidance/ccves/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification. In case of a modification to a component, NSA's CSfC Program Management Office requires a statement from NIAP that the modification does not alter the certification, or the security, of the component. Modifications which trigger the revalidation process include, but are not limited to the following: modifying the original equipment manufacturers' code (to include digitally signing the code) or not leveraging the baseline NIAP-evaluated configuration.

4.1 NETWORKS

This CP uses the following terminology to describe the various networks that comprise a Campus WLAN solution and the types of traffic present on each. The terms Red, Gray, and Black refer to the level of protection applied to the data as described below. The term Red Network refers to a network logically located behind any Inner VPN Gateway with the additional protection of an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) as illustrated in Figure 3 and Figure 4.

4.1.1 RED NETWORK

Red data consists of unencrypted classified data while Gray data consists of singly encrypted classified data. The Red network is logically located behind an Inner VPN Gateway. The networks connected to End User Devices through the Campus WLAN solution are Red networks. Red networks are under the control of the solution owner or a trusted third party. The Red network may only communicate with EUDs through the Campus WLAN solution if the EUDs operate at the same security level.

4.1.2 GRAY NETWORK

A Gray network contains classified data that has been encrypted once. The network between an Inner VPN Gateway and the WLAN Access System is a Gray network. The Gray network is physically and logically under the control of the solution owner or a trusted third party. A Campus WLAN solution compliant with this CP physically treats Gray network as a classified network even though all classified data is singly encrypted. If a solution owner's classification authority determines that the data on a Gray network is classified, perhaps by determining the Internet Protocol (IP) addresses used on the Gray

network interfaces are classified at some level, then the Campus WLAN solution described in this CP cannot be implemented, as it is not designed to ensure that such information will be afforded two layers of protection. Gray networks are either physically or cryptographically divided into two sub-networks, as follows:

- Gray Management network – The part of a Gray network that contains the management functions to run components supporting the Outer layer of WPA2, including the Outer (WPA2) tunnel Certificate Authority (CA) and the Gray admin and audit server functions. Note- the Inner and Outer CAs can both reside within the Red network.
- Gray Data network – The part of a Gray network that carries data between Inner VPN Gateway and the WLAN Access System.

4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The wireless network between the End User Device and the WLAN Access System in which data is protected with two layers of encryption (the IPsec and the WPA2 layers) is a Black network. It is important to note that the WPA2 layer can either terminate on the Access Point(s) or Wireless controller depending on which vendor product is chosen from the CSfC Components List. For WPA2 tunnels terminating at the AP, encryption standards such as IPsec, Secure Shellv2 (SSHv2), TLS, or TLS/HTTPS shall be used to encrypt data between the AP and the wireless controller. Black networks are not necessarily (and often will not be) under the control of the solution owner or can be interfered with by external third party actors.

4.2 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, that is being passed through the Campus WLAN solution. The Campus WLAN solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Black network shall be encapsulated within the Encapsulating Security Payload (ESP) protocol and WPA 2 Enterprise.

Management plane traffic is used to configure and monitor solution components. It includes the communications between a system administrator and a component, as well as the logs and other status information forwarded from a solution component to a log server, Security Information and Event Manager (SIEM) or similar repository. Management plane traffic on Red and Gray networks shall be encapsulated within the SSHv2, ESP, or TLS protocol.

Control plane traffic consists of standard protocols necessary for the network to function. Control plane traffic is typically not initiated directly on behalf of a user (unlike data traffic) or a system administrator (unlike management traffic). Many, but not all, control plane protocols operate at Layer 2 or Layer 3 of the Open Systems Interconnection (OSI) model. Examples of control plane traffic include, but are not limited to, the following:

- Network address configuration (e.g. Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery Protocol (NDP), etc.)
- Address resolution (e.g. Address Resolution Protocol (ARP), NDP, etc.)
- Name resolution (e.g. Domain Name System (DNS), etc.)
- Time synchronization (e.g. Network Time Protocol (NTP), Precision Time Protocol (PTP), etc.)
- Route advertisement (e.g. Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Border Gateway Protocol (BGP), etc.)
- Certificate status distribution (e.g. Online Certificate Status Protocol (OCSP), Hypertext Transfer Protocol (HTTP) download of Certificate Revocation Lists (CRLs), etc.)

In general, this CP does not impose detailed requirements on control plane traffic, although control plane protocols may be used in order to implement certain requirements. For example, requirements WLAN-SR-2 and WLAN-SR-3 (see Section 12.1) require that time synchronization be performed, but do not require the use of any particular time synchronization protocol or technique. Notable exceptions are for IPsec session establishment and for certain certificate status distribution scenarios where, given their impact on the security of the solution, this CP does provide detailed requirements. Unless otherwise specified in this CP, the usage of specific control plane protocols is left to the solution owner to approve, but any control plane protocols not approved by the solution owner should be disabled.

Data plane and management plane traffic are generally required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray Data network and a Gray Management network which are separate from one another, where the components on the Gray Management network are used to manage the components on the Gray Data network.

4.3 HIGH-LEVEL DESIGN

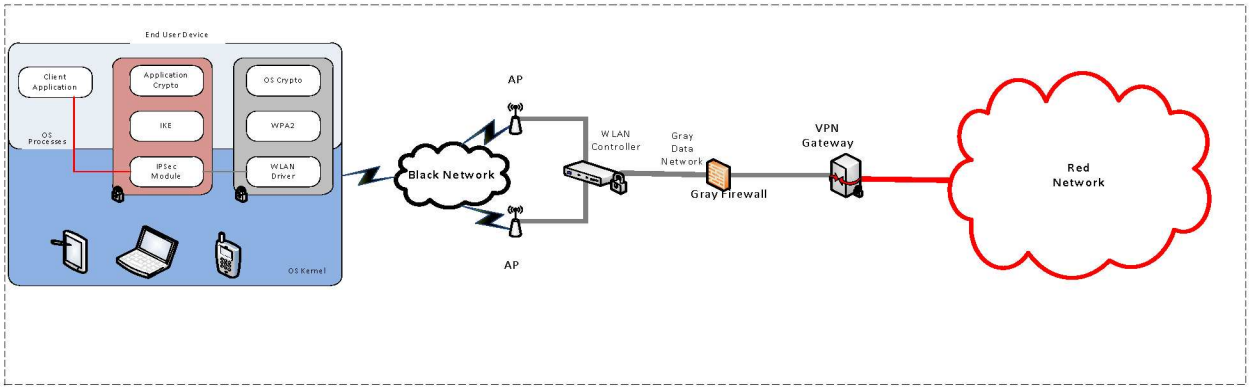

Figure 2. Campus WLAN Single Classification Implementation

The Campus WLAN CSfC solution is adaptable to support multiple capabilities, depending on the needs of the customer implementing the solution. If a customer does not have a need for supporting multiple classified networks, then those elements need not be included as part of the implementation as seen in Figure 2. Similarly, a customer may choose to implement a solution where classified information is protected as it travels over-the-air between a WLAN-enabled EUD and a WLAN infrastructure attached to a wired network of the same classification level. However, any implementation of the Campus WLAN solution must satisfy all of the applicable requirements specified in this CP, as explained in Section 10.

4.3.1 MULTIPLE SECURITY LEVELS

A single implementation of the Campus WLAN solution may support Red networks and EUDs of different security levels. The Campus WLAN solution provides secure connectivity between the Red networks and EUDs within each security level while preventing Red networks and EUDs of differing security levels from communicating with one another. This enables a customer to use the same physical wireless infrastructure to carry traffic from multiple networks.

4.3.1.1 Networks Operating at The Same Classification Level

When Red networks operate at the same classification level but at different security levels, the cryptographic separation provided by the Inner VPN Gateways is sufficient to protect against unintended data flows between security levels. Two Inner VPN Gateways for networks of different security levels will be unable to mutually authenticate with each other because they trust different Certificate Authorities (CAs) which do not have a trust relationship with one another. This prevents the establishment of an IPsec tunnel between the two components.

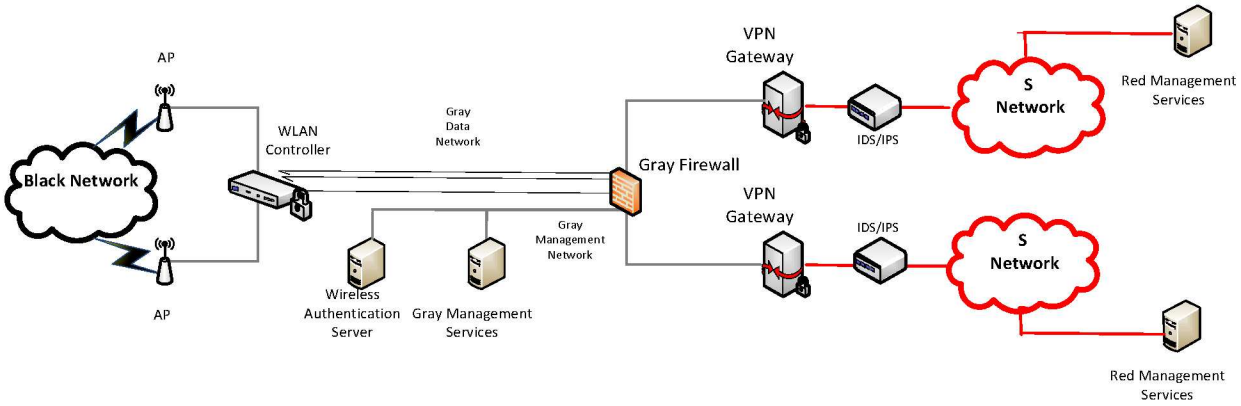

Figure 3. Campus WLAN Solution for Two Networks of the Same Classification Level

4.3.1.2 Networks Operating at Different Classification Levels

A single implementation of the Campus WLAN solution may support Red networks and EUDs of different security levels. The Campus WLAN solution provides secure connectivity between the Red networks and EUDs within each security level while preventing Red networks and EUDs of differing security levels from communicating with one another. This enables a customer to use the same wireless infrastructure to carry traffic from multiple networks.

For Red networks of different classification levels, the cryptographic separation of their traffic on a Gray network, as described in Section 4.3.1.1, is still present. However, because the consequences of an unintended data flow between different classification levels are more severe than of one with a single classification level, an additional mechanism is necessary to further guard against such a flow from occurring.

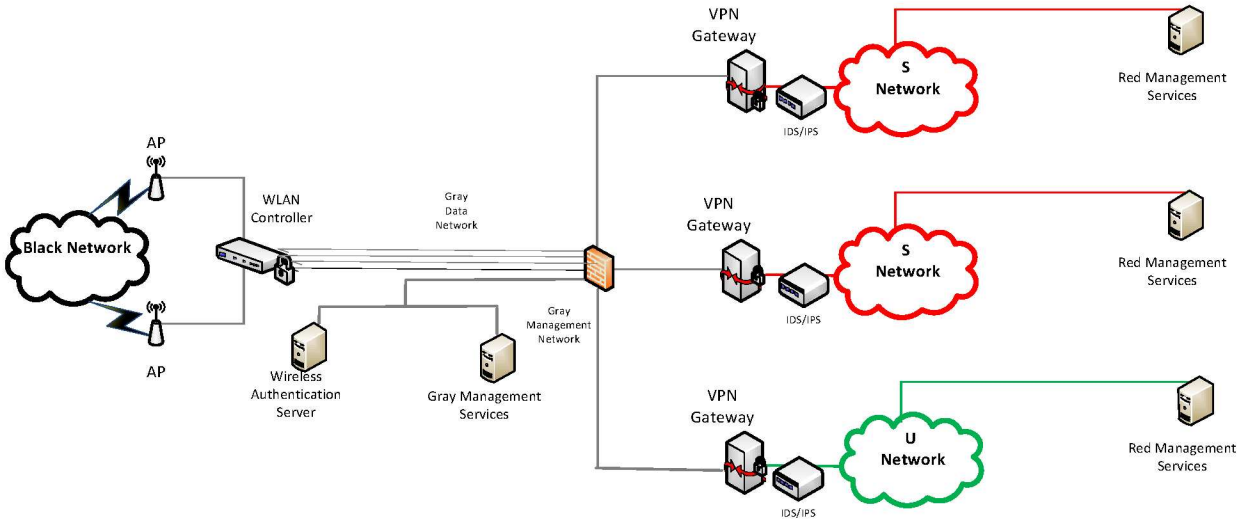

Figure 4. Campus WLAN Solution for Networks Operating at Different Classification Levels

This CP uses packet filtering within Gray networks as an additional mechanism to prevent data flows between networks of different classification levels. Any physical path through a Gray network between multiple Inner VPN Gateways supporting Red networks of different classification levels must include at least one filtering component. This filtering component restricts the traffic flowing through it based primarily on the Gray network source and destination addresses, only allowing a packet through if the source and destination components are intended to communicate with one another and dropping the packet if they are not.

When multiple classification levels are being used, it is critical to enforce proper IP address assignment and firewall rulesets. The IP address assigned must be unique to that classification level such that the end user device is only able to send and receive traffic to their respective VPN Gateway. Proper assignment of IP address and firewall rulesets is done at both the Authentication Server and WLAN access system based on either a White List or Certificate.

5 SOLUTION COMPONENTS

5.1 END USER DEVICE

The EUD is a commercial tablet, laptop computer, smartphone, or similar computing device that supports Wi-Fi connectivity options.

Figure 5 shows the software architecture of a typical EUD. The VPN client and WLAN Client run as operating system processes and exist to perform authentication and key establishment for the IPsec module and WPA2 driver respectively.

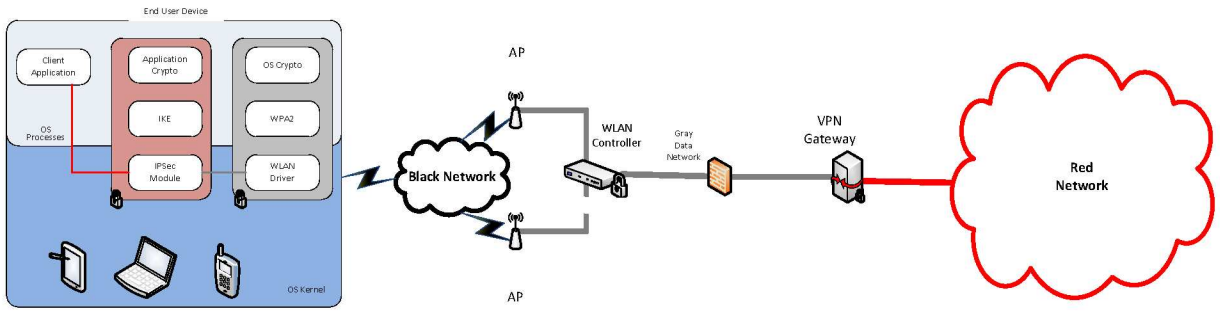

Figure 5. Campus WLAN End User Device Architecture

5.1.1 End User Device (EUD)

The EUD consists of the hardware and software components (Operating System (OS), VPN client, WLAN Client, and applications) that provide a variety of security services. The EUD is to be used exclusively within physically secure environments, such as facilities and tactical environments with physical controls considered appropriate by the Authorizing Official.

5.1.2 EUD Deployment Options

The Campus WLAN CP allows three different deployment options pertaining to the use and handling of an EUD while powered off:

- **EUD with DAR:** To implement Data-at-Rest (DAR) on an EUD, the DAR solution shall be approved by NSA – either as a tailored solution, or compliant with NSA's Data at Rest CP (DAR CP) for the protection of information classified at the level of the associated Red Network to which the EUD is connected. Specification of such a DAR solution is outside the scope of this CP, but can be found in the Data at Rest CP. The NSA requires implementing organizations to define the circumstances in which an EUD that is part of the organization's solution to be considered outside of the positive control of authorized users (i.e., "lost"). Authorizing Officials will define "positive control" and that definition should align with the intended mission and threat environment for which the solution will be deployed. Organizations must also define the circumstances in with an EUD that is a part of that organization's solution is to be considered recovered back into the positive control of authorized users (i.e., "found").

- **Thin EUD:** The EUD can be designed to prevent any classified information from being saved to any persistent storage media on the EUD. Possible techniques for implementing this include, but are not limited to: using Virtual Desktop Infrastructure (VDI) configured not to allow data from the associated Red network to be saved on the EUD, restricting the user to a non-persistent virtual machine on the EUD, and/or configuring the EUD's operating system to prevent the user from saving data locally. Since the EUD does not provide secure local storage for classified data, its user is also prohibited by policy from saving classified data to it. The EUD in this case must enable the native platform DAR protection to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration. This option is not permitted if any of the private keys or certificates stored on the EUD are considered classified by the AO. Positive control of the EUD must be maintained at all times.

- **Classified EUD:** The EUD can be used exclusively with physical security measures approved by the AO. EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices, since they can rely on the environment they are in for physical protection. If this design option is selected, then the EUDs must be treated as classified devices at all times. The EUD in this case must enable the native platform DAR protection to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration. Positive control of the EUD must be maintained at all times.

While powered on, an EUD is classified at the same level of the Red network that it communicates with through the Campus WLAN solution, since classified data may be present in volatile memory and/or displayed on screen. To mitigate the risk of accidental disclosure of classified information to unauthorized personnel while the EUD is in use, the customer must define and implement an EUD user agreement that specifies the rules of use for the system. The customer must only grant users access to an EUD after they agree to the user agreement and receive training on how to use and protect their EUD.

5.2 WLAN CLIENT

The WLAN Client (also known as WPA2 supplicant) is a software application running on the End User Device that provides management and control of the wireless connection. The products chosen to implement the WLAN Client services shall provide a base level of protection and should be able to interoperate with products from other vendors. The WLAN Client automatically establishes the WPA2 tunnel between the End User Device and the WLAN Access System using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) over 802.1X to pass Public Key device certificates for mutual authentication between the WLAN Client and WLAN Authentication Server.

5.3 VPN CLIENT

The VPN Client is a software application running on the End User Device. The products chosen to implement the VPN services shall provide cryptographic and functional services that meet or exceed the requirements listed in Section 11 for the VPN Client..

The VPN Client establishes an IPsec tunnel to the VPN Gateway. The VPN Client first performs an Internet Key Exchange (IKE) with the VPN Gateway to authenticate both parties and exchange session keys for the IPsec tunnel. Authentication is performed via mutual authentication of Public Key device certificates. When IKE completes, the IPsec tunnel is secured using the Encapsulating Security Payload (ESP).

5.4 WLAN ACCESS SYSTEM

In the context of this solution, the Access Points (AP), and the WLAN Controller compose the "WLAN Access System." These components are grouped together in this document to maintain vendor neutrality; there are a variety of WLAN Access System implementations across the vendor community.

An AP is the media converter providing a link between the WLAN Client and the WLAN Controller. The level of functionality contained within the APs is vendor-dependent. Some solutions utilize "smart" or "thick" APs that incorporate a significant amount of functionality, including cryptographic operations. In this case, the APs would be considered part of the gray network. Other solutions implement "thin" APs that merely perform the wireless/wired media conversion and push all functionality to the WLAN Controller. In this case, the APs would be considered part of the Black network. If the access point is in the Black network, it has to be physically protected and console information may need to be limited or deactivated. Console access should be addressed to secure access (i.e. tamper tape). Some vendors may produce both solutions. If WPA2 terminates on APs rather than on the WLAN Controller, then the connection between the APs and the WLAN Controller should be encrypted in a manner leveraging IPsec, SSH, TLS, or TLS/HTTPS. If WPA2 terminates on the WLAN Controller, then the WPA2 encryption is used to protect the connection between the APs and the WLAN Controller.

The WLAN Access System shall be capable of initiating and terminating multiple cryptographic tunnels to and from numerous Wireless Clients. It shall also be capable of translating EAP-TLS over 802.1X messages to EAP-TLS over Remote Authentication Dial in User Service (RADIUS) messages to pass authentication information between the WLAN Client and WLAN Authentication Server. This exchange involves a Pairwise-Master Key (PMK) that is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes the PMK to the WLAN Access System over an IPsec tunnel. The Wireless Controller and the WLAN Client use the PMK to negotiate a session key to protect the subsequent user traffic exchanged between the WLAN Client and the WLAN Access System. The WLAN Access System should operate on its own separate hardware and/or virtual device(s); depending on the vendor implementation, as mentioned above. This separation may include isolating

the switches and wiring between the APs and the controller from any existing network. At the very least, the WLAN Access System and the VPN Gateway shall operate on separate hardware. Since the WLAN Access System is deployed between the Black network and the Gray management network, it is essential to implement port filtering on the WLAN Access System's Gray network interface to prevent unauthorized traffic. Traffic should be restricted using configuration requirements stated in Section 12.6.

5.5 WLAN AUTHENTICATION SERVER

The Authentication Server is used to authenticate EUDs attempting to gain access to a Campus WLAN solution. The WLAN Authentication Server performs device authentication during the 802.1X exchange. The Wireless Client and WLAN Authentication Server perform an EAP-TLS over RADIUS exchange using the 802.1X protocol, with the WLAN Access System acting as a pass-through. As part of this exchange, a Pairwise Master Key (PMK) is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes this key to the WLAN Access System in accordance with Wireless Infrastructure Authentication requirements (WLAN-IA-1 and WLAN-IA-2) to protect the subsequent user traffic exchanged between the WLAN Client and the WLAN Access System. The WLAN Authentication Server shall operate on a separate hardware device from the WLAN Access System.

Campus WLAN solutions that support more than one enclave include additional requirements on the authentication Server to ensure that EUDs are only permitted access to the correct network that directs the traffic to the appropriate Inner VPN Gateway. There are two acceptable approaches to ensure that EUDs are only permitted access to their assigned domain. The first is to maintain a whitelist of devices and the enclave for which each device is provisioned. This whitelist can be saved in a database on the Authentication Server or can be retrieved from a separate server that resides in the Gray Network. The second approach is to utilize information in the certificate of each EUD to make the access decision. Specifically, customers can utilize fields in the Distinguished Name of the Certificate (e.g. Organizational Unit field) or utilize registered Policy Object Identifiers to assign EUDs to the appropriate domain. Use of Policy Object Identifiers (OIDs) is the preferred approach if supported by the Authentication Server and PKI.

When supporting multiple enclaves, the Authentication Server will utilize the whitelist or certificate as part of the Authentication of EUDs. Once successfully authenticated, the Authentication Server then passes the attribute information associated with the EUD's enclave to the WLAN Access System as part of the EAP-success packet. The WLAN Controller utilizes the attribute information received from the Authentication Server to ensure they are placed on the proper gray network for their enclave and receive the correct Firewall Access Control List (ACL) rules.

5.6 GRAY FIREWALL

A Campus WLAN solution that supports networks operating at different classification levels shall include a Gray Firewall, as described in Section 4.3.1.2. The primary purpose of a Gray Firewall is for filtering traffic to only allow the proper traffic to flow to and from the VPN Gateway and WLAN Controller. The Gray firewall shall be selected from the CSfC Components List and must be physically separate from the WLAN Access System and the VPN Gateways.

5.7 ADMINISTRATION WORKSTATIONS

The WLAN Access System, WLAN Authentication Server, and the WLAN Client shall have an administration workstation on the Gray Management network that allows for maintaining, monitoring, and controlling all security functionality for those devices. The administration devices for the VPN are located on the Red network. These administration devices shall also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the WLAN Access System and VPN devices. Layer 3 routing between management and data networks shall be prohibited to maintain strict separation between management and data traffic.

Administration Workstations shall be dedicated for the purposes given in the CP, and shall not be used to manage any non-CSfC solutions. As such, a dedicated virtual machine on an administration device used for non-CSfC solution cannot be used to manage CSfC solutions.

5.8 CERTIFICATE AUTHORITY

Separate Certificate Authorities (CA's) support the two layers of data-in-transit encryption (WPA2 and IPsec) in this CP. Each CA provides independent keys to the WPA2 and VPN clients respectively, and the corresponding infrastructure components:

- End User Device registration services.
- Certificate issuance services.
- Certificate renewal services.
- Certificate Revocation Services (via Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP).

Deploying separate CAs decreases the risk to the infrastructure as they provide two independent points of failure. In addition, because they provide a signer for key pairs these Certificate Authorities provide the third party trust between the users of certificates. Both the End User Device clients and the infrastructure components are issued certificates. Each has a critical role to play in verifying the trust of the other party as they connect in the wireless environment.

Certificate revocation information is made available to, and checked by, infrastructure components. The WLAN Authentication Server checks certificate revocation status prior to allowing a device to connect to the Gray network. Similarly, the VPN Gateway checks certificate revocation status prior to allowing a device to connect to the Red network.

The certificates for any compromised EUD shall be revoked, and the Outer and Inner CAs shall issue new CRLs that identify the EUD certificates as revoked. In addition, the VPN Gateway and WLAN Authentication Server shall update any local access list (e.g. whitelist) to reflect revocation of the EUD certificates. As private keys on infrastructure components are comparatively secure, the cost of making certificate revocation information available to EUDs may outweigh the benefit of doing so.

Each CA used in the solution shall have an approved Certificate Policy/ Certificate Practice Statement (CP/CPS) that is compliant with IETF RFC 3647 and addresses certificate generation, handling, distribution, storage, destruction, and key recovery and compromise recovery. Refer to NIST SP 800-57 for guidance.

The CA for the WLAN devices may be located in the Gray or Red management network and the CA for VPN devices shall be located in the Red network. If Enterprise CA's are available, they should be utilized. Otherwise a locally managed CA will need to be deployed requiring that a CA product be selected from the CSfC component list.

Each locally-operated CA shall operate on a dedicated machine, but the CAs may be operated as virtual machines (i.e., the WLAN Authentication server and the Outer CA may be Virtual Machines (VM) on the same hardware platform).

5.9 VPN GATEWAY

The VPN Gateway is an integral part of the security of the Campus 802.11 WLAN solution and is located on the gray interface of the secure wired network. Port filtering rules shall be implemented in order to prevent unauthorized traffic from reaching the Enterprise services. The VPN Gateway performs cryptographic functions related to establishing and maintaining the IPsec tunnels. It is responsible for authenticating the device certificate of the EUD's VPN Client, including checking for certificate revocation information during the IPsec VPN tunnel establishment. The VPN Gateway shall operate on its own separate hardware device.

6 CAMPUS WLAN CONFIGURATION AND MANAGEMENT

6.1 EUD PROVISIONING

Initial provisioning of campus End User Devices will be performed using enrollment capabilities hosted in the Red Network and leveraging the Outer and Inner CAs. To support different device types, it may be

necessary to support both a wireless and wired connection capabilities to the End User Device being provisioned. Since keying and secure applications needed to connect to the operational WLAN Access System have not yet been established, wireless provisioning connectivity must be performed on a separate WLAN Access System in a shielded enclosure. The provisioning process includes assigning identifiers to the devices, installing required applications, configuring the device's policy and settings (especially WPA2 and IPsec settings), and loading certificates and keying material. Prior to provisioning devices, configuration profiles are created and required device applications are obtained.

Initial provisioning (for all device types) should include—note that a specific sequence is not implied:

- **Device registration**. Collect identifying information from the End User Device, assign Government device identities for the Gray and Red domains, and update data stores (directory, inventory, and/or authorization) to include new End User Device.
- **Settings configuration**. Load configuration (within the limitations of what is supported by each device type) that implement policies on allowed and disallowed services (such as Bluetooth) and user authentication parameters (such as password length and when to lock the device). Supply other settings such as network parameters.
- **Application installation**. Load required applications, including the VPN client and enterprise client applications (there is no current support for an online application store, so all applications should be loaded during initial provisioning). If possible, unneeded applications should be removed from the device.
- **Certificate request and issuance**. Using the assigned Government device identifiers, connect to the Gray network, request certificates from the Outer CA, and load received material into the End User Device. Disconnect the device from the Gray network, connect to the Red network, request certificates from the Inner CA, and load received material into the End User Device. Note- It is possible for both CAs to reside on the Red network.

Depending on the capabilities of the EUD, the device either connects and interacts with the CAs in order to be issued certificates, or the certificates are generated and loaded onto a device storage medium from a Provisioning workstation for transfer to the End User Device. There will also be differences based on whether the End User Device generates and provides a private key for the certificate or is issued one from the CA (more secure handling and transfer is required for the latter case). Finally, some devices may require that certificate provisioning be performed using a wireless connection. In the event that a device can only support wireless certificate provisioning, the certificate provisioning must be performed in a shielded enclosure deemed appropriate by the Authorizing Official.

Once the End User Device is properly configured and certificates/keying material is in place, it is ready to be issued to a user with the final Steps of establishing user login and associating the user with the device in the registration data. Once the device is connected to the Red network, the device is classified.

6.2 MANAGEMENT OF CAMPUS WLAN SOLUTION COMPONENTS

Management of all Mobile Access Solution components is always encrypted to protect confidentiality and integrity, except in the case where components are locally managed through a direct physical connection (e.g. serial cable from the Gray Administration Workstation to the WLAN Controller). Management traffic must be encrypted with SSHv2, TLS, or IPsec.

The requirements for configuring the End User Devices in Section 12.2 can be accomplished through a variety of mechanisms. First, the EUDs can be configured utilizing a Mobile Device Management (MDM) selected from the CSfC Components List. Alternatively, the EUD can be configured utilizing a provisioning tool which enforces configuration policies during initial setup, and must be brought back to a Security Administrator to be updated. Customers can also configure End User Devices using an existing Enterprise Policy enforcement mechanism. Finally, customers can choose to utilize a hybrid approach with more then one of the above options.

7 CONTINUOUS MONITORING

The Campus WLAN CP allows customers to utilize EUDs from physical environments residing within a government secure facility. Today's technology provides increased accessibility to various networks, which present a need to continuously monitor network traffic and system log data within the solution infrastructure. This monitoring allows customers to detect, react, and report to any attacks which occur on their solution. This continuous monitoring also enables the detection of any configuration errors to Solution Infrastructure Components. At a minimum, this CP requires an Auditor to review alerts, events, and logs on a weekly basis. Operational and Strategic implementations of the Campus WLAN CP should review alerts, events, and logs on a more frequentbasis. Customers may leverage Operation Centers to perform 24 hour, 7 day a week monitoring.

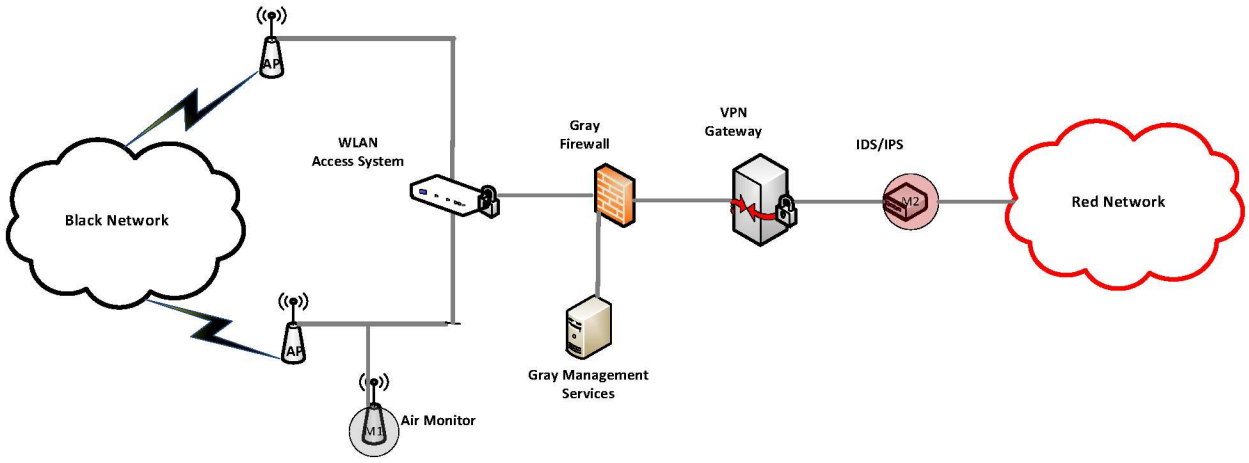

Figure 6. Campus WLAN Continuous Monitoring Points

Monitoring Point 1 - Wireless Intrusion Detection/Prevention System (WIDS/WIPS) Sensors are located not only near access points, but around the around the perimeter of the wireless network.

Monitoring Point 2 – Intrusion Detection System or Intrusion Prevention System is located between the VPN Gateway and the Red network.

7.1 Intrusion Detection and Prevention System (IDS/IPS)

The Intrusion Detection and Prevention System (IDS/IPS) is responsible for monitoring the network traffic to flow to and from the Red networks. The IDS/IPS can be either an Intrusion Detection Systems (IDS) or a Intrusion Prevention System (IPS); however, it is preferable to use an IPS to elicit real-time responses. The term IDS/IPS used in this CP will refer to both IDP and IPS technologies. The IDS/IPS will be configured to terminate the network connection or user session that is being used for an attack. The IPS shall be configured to block all access to the targeted host, service, application, or any other resource from the source of an attack. The IDS/IPS shall synchronize its time using a NTP to ensure log entries have accurate timestamps. The IDS/IPS shall be deployed on the Red network to monitor tunneled traffic being decrypted by the VPN Gateway.

Infrastructure components (servers and workstations) should be configured with Host-based IDS (HIDS) software in accordance with local policy.

7.2 Wireless Intrusion Detection System (WIDS)

A Wireless Intrusion Detection System (WIDS) consists of a group of sensors (preferably some dedicated) and a central controller working together to provide 24/7 monitoring of the wireless spectrum to detect unauthorized or malicious WLAN activity. The system can either be stand-alone or integrated into the WLAN Access System. For the stand-alone case, ideally, information between the sensors and the controller will pass over a separate network dedicated to the WIDS, but an acceptable option is to connect the sensors over a virtual LAN established over the same wired network as used by the Wireless APs. For an integrated WIDS, whether the sensors can be placed on the Wireless network or must be placed on the Gray network depends on the vendor's implementation.

7.3 Security Information and Event Management (SIEM)

The SIEM collects and analyzes log data from the WLAN Access System, Gray firewall, and IDS/IPS. Log data may be encrypted between the originating component and the Gray SIEM with SSHv2, TLS, or IPsec to maintain confidentiality and integrity of the log data. At a minimum, an auditor reviews the SIEM on a weekly basis. The SIEM is configured to provide alerts for specific events including if the WLAN Access System, Gray firewall, and IDS/IPS receive and drop any unexpected traffic, which could indicate a compromise of the WLAN Access System.

8 KEY MANAGEMENT

Campus WLAN solutions utilize asymmetric algorithms (as defined in Table 8 and Table 9) and X.509 v3 device certificates for Component authentication to establish the WPA2 layer and IPSec encryption tunnel. Each Campus WLAN solution Component contains a private authentication key and a corresponding public certificate issued by an authorized CA. In addition, a Trusted CA certificate is installed as well as any other CA signing certificates that chain to the Trusted CA, so that a trusted certificate chain is established between the Component certificate and the Trusted CA certificate. Each Campus WLAN Solution Infrastructure component also has access to revocation status of certificates (e.g. CRL or OCSP). If CRLs or OCSP is not used, other mechanisms can be implemented (e.g. whitelists) in Campus WLAN solution infrastructure components.

It is preferable for the authentication keys (public/private key pair) to be generated on the security Component, where the private keys are never exported out of the Component. If the Component cannot generate its own key pair, a dedicated management workstation is required to generate the key pair for the Component. The public keys are sent in certificate requests to the Gray and Inner CAs that create and sign authentication certificates containing the public keys. The authentication certificates are delivered to, and installed on the security Components during provisioning, along with the private keys if they were not generated on the Component. The CAs also issue signed CRLs to provide revocation status information for the certificates issued by the CAs. CRLs are transferred to CRL Distribution Points (CDPs) or On-line Certificate Status Protocol (OCSP) Responders, where the CRLs or Certificate Statuses are made available to Campus WLAN Solution Infrastructure Components.

To provide confidentiality services within Campus WLAN solutions, the Components utilize key agreement protocols (such as Elliptive Curve Diffie-Hellman Ephemeral (ECDHE)) to generate ephemeral encryption keys. The use of ephemeral encryption keys is not part of key management discussed in this section, as CAs are not required in issuing and managing these keys.

The CAs that issue authentication certificates to Campus WLAN solution Components operate either as Enterprise CAs (e.g. DoD PKI, KMI, and Agency PKI) or locally run CAs. Existing Enterprise CAs should be used whenever possible, as the advantages for using these CAs outweigh those associated with locally run CAs. Enterprise CAs have established operations, as well as Certificate Policies and Certification Practices Statements (CPSs) that customer organizations can leverage for their solution. These Enterprise CAs operate at Federal Department (e.g. DoD PKI, KMI) and Agency levels, and offer wide-scale interoperability across WLAN solutions (i.e., the certificate policies and their registered policy Object Identifiers (OIDs) are widely accepted across the Federal Department or Agency). When an Enterprise Root CA is utilized, the WLAN CP requires that at least two existing Subordinate CA's are used to issue certificates. One Subordinate CA issues certificates to WPA2 Encryption Components (known as the Outer CA) and the other CA is utilized to issue certificates to VPN Encryption Components (known as the Inner CA). To ensure that the same certificate cannot be used for authenticating both the WPA2 and IPSec tunnels, the Outer CA and Inner CA are used as trust anchors to validate the WPA2 and IPSec

tunnel authentication certificates, respectively. When multiple classified enclaves are used, each enclave will have its own Inner CA as Inner CAs cannot be shared between multiple classification levels.

For WLAN solutions requiring interoperability across a Federal Department, the Department-level Enterprise CAs should be leveraged. Examples of Department-level Enterprise CAs include the DoD PKI; the NSA Key Management Infrastructure (KMI); the National Security Systems (NSS) PKI; the Intelligence Community (IC) PKI; the Department of Homeland Security (DHS) PKI; and the Department of Energy (DoE) PKI. Enterprises like these leverage Department-level Trusted CAs which reside under the same Root CA. Trusted CAs like these can be used as trust anchors in multiple WLAN solutions throughout a Federal Department, thereby providing certificate trust interoperability across those WLAN solutions. In addition, certificates issued by Department-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Department. A user with a WLAN EUD provisioned with certificates from a Department-level Enterprise CA could possibly use their EUD in many different WLAN solutions deployed throughout a Federal Department.

Similarly, WLAN solutions requiring interoperability across a Federal Agency should leverage Agency-level Enterprise CAs. Agency-level Enterprise CAs issue certificates only to Agency personnel and Non-Person Entities (NPEs). These types of Enterprises leverage Agency-level Trusted CAs which reside under the same Root CA. This type of Trusted CAs can be used as trust anchors in multiple WLAN solutions throughout that Agency. Furthermore, certificates issued by Agency-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Agency. A user with a WLAN EUD provisioned with certificates from an Agency-level Enterprise CA could possibly use their EUD in different WLAN solutions deployed throughout that Federal Agency.

For both types of Enterprise CAs described above, a WLAN solution owner could deploy and operate independent Subordinate CAs that are issued certificates by a higher-level Enterprise CA. The benefit of this configuration is that it allows tailoring of the Subordinate CA operations to the local environment without losing the interoperability benefits gained by leveraging Enterprise CAs. However, the WLAN solution owner is responsible for defining and implementing CPSs for the Subordinate CAs that are approved by the Enterprise CA policy authorities.

Finally, WLAN solutions requiring minimal or no interoperability can deploy and operate their own locally run CAs that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability is constrained to the specific WLAN solution. Furthermore, the WLAN solution owner is required to develop and maintain CPSs that detail the operational procedures for the locally run CAs. In

addition, the customer may need to develop and maintain a higher-level Certificate Policy if one does not already exist.[1] Table 1 summarizes the differences between Enterprise and locally run CAs.

Table 1. Certificate Authority Deployment Options

CA Type	Certificate Policy	Interoperability	Operations
Department-level Enterprise	Owned and managed at the Department level (e.g. DoD PKI, NSA KMI, NSS PKI, IC PKI, DHS PKI, DoE PKI)	Department-wide	Performed by the enterprise
Agency-level Enterprise	Owned and managed at the Agency level	Agency-wide	Performed by the enterprise
Subordinate CA (Enterprise)	Owned and managed at the Department or Agency level	Department-wide or Agency-wide	Performed by the enterprise and the WLAN solution owner
Locally run (Non-Enterprise)	Owned and managed at the WLAN solution level	Constrained to the WLAN solution	Performed by the WLAN solution owner

In all CA configurations identified above, Outer CAs issue and manage authentication certificates for Gray Encryption Components and Gray Management Service Components; Inner CAs, and optionally existing CAs that support enterprise services, issue and manage authentication certificate for VPN Encryption Components and Red Management Service Components. Gray CAs can be included as either part of the Gray network or Red network. If the solution supports multiple classified enclaves the Outer CA must either be located in the Gray Management Network or in the Red Network of the highest classified enclave. Inner CAs, including existing enterprise CAs, can only be located in the Red network.

To assist the CAs in their operations, the CAs may communicate with management services (e.g., Device Managers (DMs)) deployed in the corresponding network to support enrollment and life-cycle certificate management for Campus WLAN Solution Components. Outer and Inner CAs in the Red network are limited to directly communicating with Red Management Services. Outer CAs in the Gray network are limited to directly communicating with Gray Management Services. When the CA is not located in the same network as the required management services, an AO-approved Cross Domain Solution may be utilized allowing indirect communication (for example Certificate Enrollment). The Red and Gray Management Services enable the certificate request/response process between a WLAN Solution Component and a CA. This CP recommends provisioning of WLAN Solution Components in the Red

[1] CNSSP 25 is the governing policy for PKI solutions in support of Secret Campus WLAN solutions. For Campus WLAN solutions that are higher than Secret, the Campus WLAN solution owner is required to develop a Certificate Policy that is approved by the local Approving Official (AO).

network, and that all enrollment and life-cycle certificate management be performed in accordance with the applicable Certification Practices Statements (CPSs).

This solution utilizes device authentication certificates. Device certificates and private keys used in the solution are considered Controlled Unclassified Information (CUI) (unless determined to be higher by the AO) because they are only used for mutual authentication, not for traffic encryption or granting access to classified data. While the CP enables AOs to define the classification level of Device private keys, the allowable options for use and handling of EUDs is dependent on that classification. If any of the private keys stored on an EUD are considered classified, then the solution must be treated as classified at all times or implement a NSA approved DAR Solution. Conversely, if the private keys stored on the EUD are determined to be CUI, then the EUD can also be utilized as a Thin EUD (see Section 5.1.2).

The WLAN solution described here requires certificates to establish the secure tunnels between Components. Without certificates, the network cannot function. Typically, an out-of-band method is used to issue the initial certificates to the Components. Subsequent rekeying, however, should take place over the network through this solution prior to the current key's expiration, if the Components support such a capability. The key validity period for certificates issued by locally run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to Gateways within 24 hours of CRL issuance.

9 THREATS

This section details how the required components work together to provide overall security in the solution. Section 4.3 shows the boundary of the WLAN solution for each high-level design covered by this CP.

An assessment of security was conducted on each of the high-level designs described in this CP. The assessment was made with no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data. To obtain the classified risk assessment associated with this CP, please contact the NSA via your Client Advocate.

9.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g. traffic analysis or sniffing the network) passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit across the Black network is provided by the layered IPsec tunnels. To mitigate passive attacks, two layers of Suite B encryption, Advanced Encryption Standard (AES), are employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The two Encryption Components that are used to set up the tunnels must be independent in a number of ways (see Section 10). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both tunnels.

9.2 External (Active) Threats

This threat refers to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with the intention to compromise the network or exfiltrate data, or to analyze the design of the network or system for future attacks. Adversaries could gain access to a WLAN Access System or EUD, and then exploit or compromise other devices on the network. DoS or Distributed DoS (DDoS) attacks compromise availability of the system, degrading/disrupting secure communication across the Wireless Infrastructure. Further external threat actions would include; social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

9.2.1 Rogue Traffic

One method for detecting rogue traffic from an external attack as it attempts to pass through WLAN Components is by having the port filtering native to each component enabled and configured to audit and log any traffic that is not one of the formats described in the configuration. This will allow the Auditor(s) and/or the Security Administrator(s) to detect whether the WLAN Access System has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of misconfigured WLAN components.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on Red and Gray Management networks to ensure that the VPN Gateway configurations are not changed without the knowledge of Auditors and Security Administrators. Auditors also ensure through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of the VPN Gateway misconfigurations.

End User Devices (EUDs) are protected from rogue traffic through the use of traffic filtering rules configured on their interfaces connected to Black networks to drop any traffic not necessary for connecting to the necessary WLAN Access System.

9.2.2 Malware and Untrusted Updates

Administration Workstations and locally run CAs for Inner Tunnel Components shall be distinct and physically separate from the Administration Workstations and locally run CAs for Outer Tunnel Components. This separation minimizes the potential for malware on a single device to impact components supporting both Inner and Outer WLAN solution tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

9.2.3 Denial of Service

Denial of Service (DoS) attack risks cannot be completely mitigated. WLAN solutions in compliance with this CP requires that the Gray firewall drop all packets that are not Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), or other approved protocols on the appropriate interfaces, which significantly reduces the potential for flooding attacks.

A single encryption component failure is likely to result in a DoS condition. One assumption underlying this solution is that high assurance of availability is not required. If availability is critical for the customer, protection against DoS attacks can be achieved through network redundancy and instituting DoS response procedures when loss of availability is detected.

9.2.4 Social Engineering

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and are already discussed.

9.3 Insider Threats

This threat refers to an authorized or cleared person or group of people with physical or logical access to the network or system who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in a loss of data integrity, unintentional access to an unauthorized system or network, willingly changing the configuration of an EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing the network and systems to viruses or malware, cross-contaminating a system or network with data from a higher

classification to a lower classification (e.g. Secret data to an Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 14). In addition, logging and auditing of security critical functionality (see Section 12.13) is required. Also, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on Encryption Components, firewalls, and EUDs are configured to block traffic leaving the internal network that does not go through the Encryption tunnels.

Additionally, organizations concerned about users misbehaving when connected remotely may wish to restrict the use of EUDs to those deemed sufficiently trustworthy.

9.4 Supply Chain Threats

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the Information and Communication Technology (ICT) components embedded in the systems and networks upon which the ability to perform U.S. Government missions rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component; they are only able to provide assurances based on their reliance of established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor, retailer, reseller, or shipper and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify, and is increasingly more difficult to prevent or protect against, since vendors build products containing components manufactured by subcontractors. It is often difficult to determine where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates,

distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance). Even after selecting components from the CSfC Components List and utilizing a rigorous acquisition process, an AO must perform due diligence when integrating commercial components for mission operations.

Doctrinal requirements are placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks. To further mitigate Supply Chain Threats implementing organizations should utilize the following guidance:

- Establish an ICT SCRM program which conforms to applicable policy based on external and organizational requirements and constraints. The ICT SCRM program should be integrated into the organizational business and mission processes.
- Assess all aspects of the performance of potential vendors, not only the product quality, cost, and performance, but also supply chain risk factors of vendor selection. These risk factors include political ties to foreign governments, citizenship of employees, partner affiliations, employee clearance levels, and location of suppliers and sub-suppliers.
- Ensure that each component selected from the CSfC Components List go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component (see CNSSD 505 Supply Chain Risk Management and Intelligence Community Directive (ICD) 731 Supply Chain Risk Management).
- Conduct a Criticality Analysis by which mission-critical functions and components are identified and prioritized with respect to improving acquirer practices (see Defense Acquisition Guidebook, Chapter 13).

Supply chain risk management is a critical consideration in acquiring commercial products. Even after selecting components from the CSfC Components List and utilizing a rigorous acquisition process an AO must do their due diligence as composed commercial products are integrated into mission operations.

9.5 Integrator Threats

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different

from a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the WLAN solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution. More information on the NSA's list of trusted integrators can be found on the NSA CSfC Website in the "Criteria For CSfC Integrators" section at this link: https://www.nsa.gov/ia/programs/csfc/index.shtml.

10 REQUIREMENTS OVERVIEW

The following five sections (Sections 11 through 15) specify requirements for implementations of WLAN solutions compliant with this CP. However, not all requirements in the following sections will apply to each compliant solution.

10.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

In some cases, multiple versions of a requirement may exist in this CP. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible solution owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Optional' in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold / Objective" column indicates that the Threshold equals the Objective (T=O).

Requirements that are listed as Objective in this CP may become Threshold requirements in a future version of this CP. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this CP.

10.2 Requirements Designators

Each requirement defined in this CP has a unique identifier consisting of the prefix "WLAN," a digraph that groups related requirements together (e.g. "KM"), and a sequence number (e.g. 11).

Table 2 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

Table 2. Requirement Digraph

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 11	Table 3
SR	Overall Solution Requirements	Section 12.1	Table 4
EU	End User Device Requirements	Section 12.2	Table 5
WC	WLAN Client Configuration Requirements	Section 12.3	Table 6
WL	Wireless Link Requirements	Section 12.3	Table 7
CR	Configuration Requirements for VPN Components	Section 12.4	10.3 Table 10Configuration Requirements for VPN Components and VPN Client Table 10
WS	WLAN Access System Configuration Requirements	Section 12.5	Table 11
IA	Wireless Infrastructure Authentication Requirements	Section 12.5	Table 12
AA	Wireless Authentication and Authorization Requirements	Section 12.5	Table 13
WA	Wireless Authentication Server to WLAN Client Requirements	Section 12.5	Table 14
PF	Port Filtering Requirements for Solution Components	Section 12.6	Table 15

Digraph	Description	Section	Table
PR	End User Device (EUD) Provisioning Requirements	Section 12.7	Table 16
VG	VPN Gateway Requirements	Section 12.8	Table 17.
WI	Wireless Intrusion Detection Configuration Requirements	Section 12.9	Table 18
CM	Configuration Change Detection Requirements	Section 12.10	Table 19
DM	Device Management Requirements	Section 12.11	Table 20
MR	Continuous Monitoring Requirements	Section 12.12	Table 21
AU	Auditing Requirements	Section 12.13	Table 22
KM	Key Management Requirements	Section 12.14	Table 23 Table 24 Table 25 Table 26
FW	Gray Firewall Requirements	Section 12.15	Table 27
GD	Requirements for the Use and Handling of Solutions	Section 13.1	Table 28
RP	Incident Reporting Requirements	Section 13.2	Table 29
GD	Role-Based Personnel Requirements	Section 14	Table 30
TR	Test Requirements	Section 15.1	Table 31

11 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 3. Production Selection Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PS-1	The product used for the VPN Gateway(s) shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	T=O	
WLAN-PS-2	The products used for any WLAN Access System shall be chosen from the list of WLAN Access Systems on the CSfC Components List.	T=O	
WLAN-PS-3	The products used for any WLAN Client shall be chosen from the list of Mobile Platforms on the CSfC Components List. All validated Mobile Platform components include validated WLAN Client implementations.	T=O	
WLAN-PS-4	Products used for Mobile Platform EUDs shall be chosen from the list of Mobile Platforms on the CSfC Components List.	T=O	
WLAN-PS-5	The products used for the Inner VPN Client shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	T=O	
WLAN-PS-6	Intrusion Prevention Systems (IPS) shall be chosen from the list of IPS on the CSfC Components List.	O	Optional
WLAN-PS-7	Products used for the Gray firewall shall be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	T=O	
WLAN-PS-8	The Inner VPN Gateway and the WLAN Access System shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PS-9	The WLAN Access System, Gray Firewall, Inner VPN Gateway shall use physically separate components, such that no component is used for more than one function.	T=O	
WLAN-PS-10	The Outer and Inner CAs shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. or Utilize a Enterprise PKI approved by the AO.	T=O	
WLAN-PS-11	The EUD's VPN Client and WLAN Client shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	T=O	
WLAN-PS-12	The cryptographic libraries used by the WLAN Access System and the Inner VPN Gateway shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	Optional
WLAN-PS-13	Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	T=O	
WLAN-PS-14	Components shall be configured to use the NIAP-certified evaluated configuration.	T=O	

12 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next Step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the WLAN solution.

CPs provide architecture and configuration information that allows customers to select COTS products from CSfC component lists for their solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data. CSfC component lists consist of eligible COTS products identified by model/version numbers that have met appropriate Protection Profile requirements.

This section contains requirements applicable to the Campus WLAN solution components. In this section, a series of overarching architectural requirements are given for maximizing the independence between the components within the solution. This independence will increase the level of effort required to compromise this solution.

The products that are approved for use in this solution will be listed on the CSfC Components List on the IAD/CSfC website (http://nsagov.nsa.gov/ia/programs/csfc_program/index.shtml). No single commercial product shall be used to protect classified information. The only approved methods for using COTS products to protect classified information in transit on a Campus WLAN follow the requirements outlined in this CP.

Once the products for the solution are selected, each product shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.)

12.1 Overall Solution Requirements

Table 4. Overall Solution Requirements (SR)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-SR-1	Default accounts, passwords, community strings and other default access control mechanisms for all Campus WLAN components shall be changed or removed.	T=O	
WLAN-SR-2	The time of day on the VPN Gateway shall be synchronized to a time source located in the Red network.	T=O	
WLAN-SR-3	The time of day on the WLAN Authentication Server, the WLAN Controller and Gray network Components shall be synchronized to a time source located in the Gray Management network.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-SR-4	All components shall be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	T=O	
WLAN-SR-5	Solution Components shall receive virus signature updates as required by the local agency policy and the AO.	T=O	
WLAN-SR-6	The only approved physical paths leaving the Red network shall be through a WLAN solution in accordance with this CP or via an AO-approved solution for protecting data in transit.[2]	T=O	

12.2 End User Devices Requirements

Table 5. End User Device (EU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-1	The EUD shall restrict configuration (Service Set Identifier (SSID) and authentication mechanism) of authorized WLANs to authorized administrators.	T=O	
WLAN-EU-2	The EUD shall be configured with separate authentication and privileges for administrator and user roles.	T=O	
WLAN-EU-3	The EUD shall be loaded with only AO-approved software.	T=O	
WLAN-EU-4	The EUD shall restrict installation and removal of software to authorized administrators.	T=O	
WLAN-EU-5	The EUD shall require a user to log in prior to granting access to any EUD functionality.	T=O	
WLAN-EU-6	The EUD shall be configured to limit the number of incorrect logins per an AO-approved period of time either by erasing the configuration and data stored on the device or by prohibiting login attempts for a AO-approved period of time.	T=O	

[2] In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) product. In particular, it is acceptable for a given site to have both an egress path via an NSA-certified product and an egress path via a CSfC Solution conforming to a CP.

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-7	Rekeying of an EUD's certificates and associated private keys shall be done through re-provisioning prior to expiration of keys.	T	WLAN-EU-8
WLAN-EU-8	Rekeying of an EUD's certificates and associated private keys shall be done over the WLAN solution network prior to expiration of keys.	O	WLAN-EU-7
WLAN-EU-9	An EUD shall be deauthorized from the network and submitted for Forensic Analysis if suspected of being compromised.	T=O	
WLAN-EU-10	An EUD should be destroyed only if it has been determined to be compromised through Forensic Analysis.	T=O	
WLAN-EU-11	Users of EUDs shall successfully authenticate themselves to the services they access on their respective Red network using an AO-approved method.	T=O	
WLAN-EU-12	Red network services shall not transmit any classified data to EUDs until user authentication succeeds.	T=O	
WLAN-EU-13	The EUD shall lock the screen and require user re-authentication after an AO-approved period of inactivity.	T=O	
WLAN-EU-14	All EUD Users shall sign an organization-defined user agreement before being authorized to use an EUD.	T=O	
WLAN-EU-15	All EUD Users shall receive an organization-developed training course for operating an EUD prior to use.	T=O	
WLAN-EU-16	At a minimum, the organization-defined user agreement shall include each of the following: Consent to monitoring Operations Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA Training • Verification of appropriate clearance Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-17	EUDs shall be dedicated for use solely in the WLAN solution, and not used to access any resources on networks other than the Red network it communicates with through the two layers of encryption.	T=O	
WLAN-EU-18	The EUD shall disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	T=O	
WLAN-EU-19	The EUD shall have all cellular access disabled.	T=O	
WLAN-EU-20	The EUD shall have all network and wireless interfaces disabled except for 802.11.	T=O	
WLAN-EU-21	The EUD shall have all cellular services disabled.	O	Optional
WLAN-EU-22	All EUDs shall have their certificates revoked and resident image removed prior to disposal.	T=O	
WLAN-EU-23	Passwords for user-to-device authentication shall be a minimum of 4 alpha-numeric case sensitive characters.	T=O	
WLAN-EU-24	The native platform DAR protection shall be enabled[3].	T=O	
WLAN-EU-25	EUDs shall use a unique X.509 v3 device certificate, signed by the Outer CA, for mutual authentication with the Wireless Access System.	T=O	
WLAN-EU-26	VPN EUDs shall use a unique X.509 v3 device certificate, signed by the Inner CA, for mutual authentication with the VPN Gateways.	T=O	
WLAN-EU-27	The EUD maximum password lifetime shall be less than 181 days.	T=O	
WLAN-EU-28	The EUD screen shall lock after an AO approved period of inactivity.	T=O	
WLAN-EU-29	The EUD shall perform a wipe of all protected data after 10 or less authentication failures.	T=O	
WLAN-EU-30	During provisioning, all unnecessary keys shall be destroyed from the EUD secure key storage.	T=O	
WLAN-EU-31	During provisioning, all unnecessary X.509 certificates shall be removed from the EUD Trust Anchor Database.	T=O	

[3] If the WLAN Solution is implemented in conjuction with a NSA approved DAR Solution, then all applicable DAR CP requirements must also be implemented.

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-32	All display notifications shall be disabled while in a locked state.	O	Optional
WLAN-EU-33	USB mass storage mode shall be disabled on the EUDs.	O	Optional
WLAN-EU-34	USB data transfer shall be disabled on the EUDs.	O	Optional
WLAN-EU-35	Prior to installing new applications, the application digital signature shall be verified.	T=O	
WLAN-EU-36	The EUD shall be configured to only permit connections to whitelisted SSIDs.	T=O	
WLAN-EU-37	The EUD shall be configured to only permit connection to SSIDs signed by the Outer CA.	T=O	
WLAN-EU-38	The EUD shall only display whitelisted SSIDs to the user.	T=O	
WLAN-EU-39	The EUD shall only permit the execution of Applications on a whitelist.	O	Optional

12.3 Configuration Requirements for the WLAN Client

Table 6. WLAN Client (WC) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WC-1	The WLAN Client tunnel shall be established at EUD start-up.	T=O	
WLAN-WC-2	The WLAN Client shall authenticate the identity of the WLAN Authentication Server by verifying that the WLAN Authentication Server's certificate chain is rooted by the WLAN trusted root Certificate Authority.	T=O	
WLAN-WC-3	The WLAN Client shall be configured to authenticate only specific servers through setting the client to accept only a WLAN Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	T=O	
WLAN-WC-4	A unique device certificate shall be loaded into the WLAN Client along with the corresponding CA (signing) certificate.	T=O	
WLAN-WC-5	The device certificate shall be used for WLAN Client authentication during EAP-TLS.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WC-6	The WLAN Client shall provide the user with advance warning that the WLAN Client's device certificate is due to expire.	T=O	
WLAN-WC-7	The WLAN Client shall negotiate new session keys with the WLAN Access System at least once per hour.	T=O	
WLAN-WC-8	The WLAN Client shall be prevented from using ad hoc mode (client-to-client connections).	T=O	
WLAN-WC-9	The WLAN Client shall be prevented from using network bridging.	T=O	
WLAN-WC-10	The WLAN Client shall only associate with authorized Access Points based on attributes such as SSID or Whitelist and enforce based on the Certificate presented by the Authentication Server during mutual authentication.	T=O	
WLAN-WC-11	The WLAN Client shall verify that the WLAN Authentication Server X.509v3 certificate contains the TLS Web Server Authentication Object Identifier (OID) (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension.	T=O	
WLAN-WC-12	The device certificate for the WLAN Client shall contain an extendedKeyUsage field indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2).	T=O	
WLAN-WC-13	The WLAN Client shall be managed from the Gray Management Network accessible via the Campus WLAN.	T=O	

Table 7. Wireless Link (WL) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WL-1	The WLAN Client and the WLAN Access System shall use protocols and algorithms selected from Table 8 that are approved to protect the highest classification level of the Red Network data.	T=O	
WLAN-WL-2	The WLAN Client and the WLAN Access System shall operate in WPA2-Enterprise mode.	T=O	
WLAN-WL-3	The WLAN Client and the WLAN Access System shall use integrity algorithms that implements NIST AES Key Wrap with HMAC-SHA-384-128 as specified in Section 11 of IEEE 802.11-2012.	T=O	
WLAN-WL-4	If WPA2 terminates on APs then all data between the Access Point(s) and Wireless controller shall be encrypted using IPsec, SSHv2, TLS, or TLS/HTTPS .	T=O	

Table 8. IPSec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite 2	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature) (Threshold – Unclassified Only)	RSA 3072	FIPS PUB 186-4
Authentication (Digital Signature) (Objective) (Threshold – All Classified NSS)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20) or DH 3072	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Top Secret	

Table 9. WPA2 Encryption and EAP-TLS (Approved Algorithms for Classified)

Security Service	Algorithm Suite 2	Specifications
Confidentiality (Encryption)	AES-128-CCMP (Threshold) AES-256-GCMP (Objective)*	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)*	IETF RFC 5216 IETF RFC 5246

12.4 Configuration Requirements for VPN Components and VPN Client

Table 10. Configuration Requirements (CR) for VPN Components

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CR-1	The VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table 8 that are approved to protect the highest classification level of the Red Network data.	T=O	
WLAN-CR-2	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any WLAN Access System Component and VPN Gateway Component, shall not be used for establishing Security Associations (SAs).	T	WLAN-CR-3
WLAN-CR-3	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any WLAN Access System Component and Inner VPN Component, shall be removed.	O	WLAN-CR-2
WLAN-CR-4	All IPsec connections shall use IETF standards compliant IKE implementations (RFC 5996 or RFC 2409).	T=O	
WLAN-CR-5	All Outer and Inner VPN Components shall use Cipher Block Chaining for IKE encryption.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CR-6	All WLAN Components and VPN Gateway shall use Cipher Block Chaining for ESP encryption with a Hash-based Message Authentication Code (HMAC) for integrity.	T	WLAN-CR-7
WLAN-CR-7	All WLAN Components and VPN Gateway shall use Galois Counter Mode for ESP encryption.	O	WLAN-CR-6
WLAN-CR-8	All WLAN Components and VPN Gateway shall set the IKE SA lifetime to at most 24 hours.	T=O	
WLAN-CR-9	All WLAN Components and VPN Gateway shall set the ESP SA lifetime to at most 8 hours.	T=O	
WLAN-CR-10	Each VPN Client shall use a unique private key for authenticating to the VPN Gateway.	T=O	
WLAN-CR-11	The VPN Client shall provide the user with advance warning that the VPN client certificate is due to expire.	T=O	
WLAN-CR-12	The VPN Client shall be configured to prohibit split tunneling.	T=O	

12.5 Configuration Requirements for the WLAN Access System

The WLAN Access System is involved in establishing two encrypted channels. Once WLAN Authentication Server passes the PMK to the WLAN Access System, the WLAN Access System establishes an encrypted channel with the WLAN Client for passing data. The WLAN Access System acts as a pass-through for the initial authentication exchange between the WLAN Client and the WLAN Authentication Server during which the PMK is securely negotiated.

Table 11. WLAN Access System (WS) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WS-1	The WLAN Access System shall act as an EAP-TLS pass-through between the WLAN Client and WLAN Authentication Server for authentication and key establishment.	T=O	
WLAN-WS-2	The WLAN Access System shall negotiate new session keys with the WLAN Clients at least once per hour.	T=O	
WLAN-WS-3	Authentication performed by the WLAN Access System shall include a check that device certificates are authorized. This check may use a CRL, OCSP, or Whitelist.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WS-4	A unique device certificate shall be loaded into the Authentication Server along with the corresponding CA (signing) certificate.	T=O	
WLAN-WS-5	When supporting multiple enclaves, the WLAN Access System shall assign a firewall ACL to EUDs based on the attribute information provided by the Authentication Server.	T=O	
WLAN-WS-6	When supporting multiple enclaves, the WLAN Access System shall route EUD traffic over the appropriate interface based on attribute information provided by the Authentication Server.	T=O	
WLAN-WS-7	When supporting multiple enclaves, the WLAN Access System shall utilize unique physical internal interfaces for each enclave of the solution (e.g. VLAN Trunking of multiple enclaves is not permitted).	T=O	

Table 12. Wireless Infrastructure Authentication (IA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-IA-1	The WLAN Access System and the WLAN authentication server shall be physically co-located in the same rack and directly connected to each other.	T	WLAN-IA-2
WLAN-IA-2	Communications between the WLAN Access System and the WLAN Authentication Server shall be established with either an IPsec tunnel (using either IKEv1 orIKEv2) or TLS/RADsec connection.	O	WLAN-IA-1
WLAN-IA-3	The IKE exchange and IPsec tunnel between the WLAN Access System and the WLAN Authentication Server shall use protocols and algorithms selected from the Algorithm Suite in Table 8.	T=O	
WLAN-IA-4	The ESP SA tunnel between the WLAN Access System and the WLAN Authentication Server shall be ESP using Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with a SHA-based HMAC for integrity .	T	WLAN-IA-5
WLAN-IA-5	The ESP SA tunnel between the WLAN Access System and the WLAN Authentication Server shall be ESP use AES in Galois Counter Mode (GCM) mode.	O	WLAN-IA-4

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-IA-6	The lifetime of the IKE SA between the WLAN Access System and the WLAN Authentication Server shall be set to 24 hours.	T=O	
WLAN-IA-7	The lifetime of the ESP SA between the WLAN Access System and the WLAN Authentication Server shall be set to 8 hours or less.	T=O	
WLAN-IA-8	The WLAN Access System and the WLAN Authentication Server shall authenticate one another using X.509 version 3 certificates.	O	WLAN-IA-9
WLAN-IA-9	The WLAN Access System and the WLAN Authentication Server shall authenticate one another using pre-shared keys.	T	WLAN-IA-8
WLAN-IA-10	Composition rules for a pre-shared key between the WLAN Access System and the WLAN Authentication Server shall be set by the Security Administrator.	T=O	
WLAN-IA-11	The entropy of a pre-shared key between the WLAN Access System and the WLAN Authentication Server shall be a minimum of 256 bits.	T=O	
WLAN-IA-12	The IKE exchange between the WLAN Access System and the WLAN Authentication Server shall use algorithms selected from Table 8.	T=O	

Table 13. Wireless Authentication and Authorization (AA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AA-1	The WLAN Authentication Server and WLAN Client shall perform mutual authentication using EAP-TLS with device certificates.	T=O	
WLAN-AA-2	The WLAN Client and the WLAN Authentication Server shall use the AES key size and mode from for WPA2 Enterprise from the Threshold Section of Table 9.	T	WLAN-AA-3
WLAN-AA-3	The WLAN Client and the WLAN Authentication Server shall use the AES key size and mode from for WPA2 Enterprise from the Objective Section of Table 9.	O	WLAN-AA-2
WLAN-AA-4	The WLAN Client and WLAN Authentication Server shall use the EAP-TLS Ciphersuite from Table 9.	T=O	

Table 14. Wireless Authentication Server (WA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WA-1	The WLAN Authentication Server (AS) shall ensure it uses the most current CRL to check revocation status of the WLAN Client Certificate. If CRL does not exist, is invalid or has expired, authentication of the EUD will fail.	T=O	
WLAN-WA-2	The device certificate for the WLAN Authentication Server shall contain an extendedKeyUsage field indicating support for Server Authentication (Object Identifier (OID) 1.3.6.1.5.5.7.3.1).	T=O	
WLAN-WA-3	The WLAN Authentication Server shall only successfully authenticate a WLAN Client if the WLAN Client's certificate contains an extendedKeyUsage field indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2).	T=O	
WLAN-WA-4	The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the Distinguished Name or the Subject Alternate Name contained in the WLAN Client's certificate.	T=O	
WLAN-WA-5	The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate is not expired.	T=O	
WLAN-WA-6	The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate chain is rooted by the WLAN trusted root Certificate Authority.	T=O	
WLAN-WA-7	The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate is not expired.	T=O	
WLAN-WA-8	The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate is not revoked.	T=O	
WLAN-WA-9	When supporting multiple enclaves, the AS shall verify that the Common Name presented by the EUD certificate is included on a whitelist tied to an enclave.	T	WLAN-WA-10
WLAN-WA-10	When supporting multiple enclaves, the AS shall verify that the certificate presented includes information in the Distinguished Name or Policy OIDs that ties the device to a single enclave.	O	WLAN-WA-9

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WA-11	When supporting multiple enclaves, the AS shall provide attribute information on the appropriate enclave for the EUD to the Wireless Access System.	T=O	
WLAN-WA-12	The AS shall log all successful authentication attempts.	T=O	
WLAN-WA-13	The AS shall log all failed authentication attempts.	T=O	

12.6 Port Filtering Requirements

Port Filtering is composed of a component configured with Access Control Lists (ACLs). The system ensures that the traffic flowing to and from each component on the network is appropriate for the functionality of the component within the Campus WLAN solution.

Table 15. Port Filtering (PF) Requirements for Solution Components

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PF-1	All Components within the Solution shall have all network interfaces restricted to the fewest address ranges, ports, and protocols possible.	T=O	
WLAN-PF-2	All Components within the Solution shall have all unused network interfaces disabled.	T=O	
WLAN-PF-3	For all interfaces connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only EAP-TLS, IKE, IPsec, and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed shall be blocked.	T=O	
WLAN-PF-4	Any service or feature that allows an EUD to contact a third party server (such as one maintained by the manufacturer) shall be blocked.	T	WLAN-PF-6
WLAN-PF-5	Any service or feature that allows an EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled.	O	WLAN-PF-5
WLAN-PF-6	The WLAN Access System shall block all data ports and IP addresses on their Gray Management network interface that are not necessary for the management of the WLAN Access System.	T=O	
WLAN-PF-7	Interfaces of the WLAN Access System shall be based on known MAC addresses of EUDs to further protect against unknown WLAN Clients.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PF-8	Traffic filtering rules on the EUD shall be applied based on known VPN Gateway addresses or address range to further protect against unknown IPsec traffic.	T=O	
WLAN-PF-9	The internal interface of the Inner VPN Gateway shall prohibit all management plane traffic (e.g. SSH, Remote Desktop Protocol (RDP), Telnet) originating from EUDs destined for the Red Network.	T=O	
WLAN-PF-10	The internal interface of the Inner VPN Gateway shall prohibit traffic destined for the Red Management Network (e.g. Red Management Network IP addresses) originating from End User Devices.	T=O	

12.7 End User Device (EUD) Provisioning Requirements

Table 16. EUD Provisioning Requirements (PR)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PR-1	A Provisioning WLAN using WPA2-PSK authentication and encryption shall be established on the Red network to support wireless provisioning of EUDs.	T	
WLAN-PR-2	The Provisioning WLAN on the Gray Management Network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T	
WLAN-PR-3	The Provisioning WLAN on the Red network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T	
WLAN-PR-4	EUDs shall be provisioned over the Provisioning WLANs.	T	WLAN-PR-5
WLAN-PR-5	EUDs shall be provisioned over wired connections.	O	WLAN-PR-4
WLAN-PR-6	When a EUD has been successfully provisioned, its identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) shall be recorded in authorization databases accessible to the WLAN Authentication Server and VPN Gateway.	T=O	
WLAN-PR-7	EUDs shall be provisioned to be disabled by having their certificates revoked.	T=O	
WLAN-PR-8	The EUD shall be loaded with an authorized software build during provisioning.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PR-9	The EUD shall be loaded with WLAN and VPN configuration profiles during provisioning.	T=O	
WLAN-PR-10	Strong passwords for the EUD shall be used to comply with the requirements of the policy established by the AO.	T=O	
WLAN-PR-11	Services not authorized by the AO shall be disabled during the provisioning of the EUD.	T=O	

12.8 Configuration of the VPN Gateway

Table 17. VPN Gateway (VG) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-VG-1	A unique device certificate shall be loaded onto each VPN Gateway along with the corresponding CA (signing) certificate.	T=O	
WLAN-VG-2	The private key stored on VPN Gateway shall not be accessible through any interface.	T=O	
WLAN-VG-3	The VPN Gateway shall be configured to prohibit split tunneling	T=O	
WLAN-VG-4	VPN Gateway authentication shall include a check that the certificate is authorized, which can include a Certificate Revocation List (CRL) or whitelist.	T=O	
WLAN-VG-5	The VPN Gateway authentication shall include a validation check on the Distinguished Name or Subject Alternate Name in the VPN Client's X.509v3 device certificate against a database.	T=O	
WLAN-VG-6	The VPN Gateway authentication shall include a check that the certificate is not expired.	T=O	

12.9 Configuration Requirements for Wireless Intrusion Detection System (WIDS)

Table 18. Wireless IDS (WI) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-1	The WIDS shall use a whitelist of all authorized wireless network devices (i.e. Access points and EUDs) and allow for administrator modifications.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-2	The WIDS shall detect access points which are not on the whitelist, but are within the coverage area of the WIDS sensors.	T=O	
WLAN-WI-3	The WIDS shall detect EUDs which are not on the whitelist, but are within the coverage area of the WIDS sensors.	T=O	
WLAN-WI-4	The WIDS shall allow for administrator-defined rogue AP detection classification rules.	T=O	
WLAN-WI-5	The WIDS shall detect if a rogue AP is connected via wire to the network.	O	Optional
WLAN-WI-6	The WIDS shall distinguish between the mere presence of unauthorized wireless hardware within the coverage area of the WIDS sensors and an attempt to use that hardware to gain access to the wireless network.	T=O	
WLAN-WI-7	All communication between WIDS components shall be done via a secure connection (using SSHv2, IPSec, TLS, or TLS/HTTPS).	O	Optional
WLAN-WI-8	The WIDS shall geographically locate all wireless hardware operating in the coverage area of the WIDS sensors.	O	Optional
WLAN-WI-9	The WIDS shall be configured to monitor all 802.11 frame types and subtypes between unauthorized EUDs and authorized APs.	T=O	
WLAN-WI-10	The WIDS shall be configured to monitor all 802.11 frame types and subtypes between unauthorized APs and authorized EUDs.	T=O	
WLAN-WI-11	The WIDS shall be configured to monitor all 802.11 frame types and subtypes between authorized APs and authorized EUDs.	T=O	
WLAN-WI-12	The WIDS shall allow for capturing the raw frames that triggered an alert as well as options on how long to continue capturing.	O	Optional
WLAN-WI-13	The WIDS shall monitor and analyze traffic from all 802.11 channels within the 2.4Ghz and 4.9/5.0Ghz bands including those outside regulatory domain.	T=O	
WLAN-WI-14	The WIDS shall monitor and analyze traffic from all 802.11 channels within the 3.6Ghz and 60Ghz bands.	O	Optional
WLAN-WI-15	The WIDS shall detect the use of unauthorized wireless channels by whitelisted devices.	T=O	
WLAN-WI-16	The WIDS shall determine which SSIDs are permitted on the network based on whitelisted APs or have the ability to be configured with a list of permitted SSIDs.	T=O	
WLAN-WI-17	The WIDS shall detect whitelisted APs using SSIDs not permitted on the network (including hidden SSID).	T=O	
WLAN-WI-18	The WIDS shall detect and log unauthorized APs broadcasting the same SSID as a whitelisted AP.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-19	The WIDS shall detect whitelisted EUDs associating to SSIDs not permitted on the network (including hidden SSID).	T=O	
WLAN-WI-20	The WIDS shall be configured to detect whitelisted devices attempting to use unauthorized authentication methods.	T=O	
WLAN-WI-21	The WIDS shall detect whitelisted devices attempting to use unauthorized encryption schemes.	T=O	
WLAN-WI-22	The WIDS shall be configured to process 802.11 traffic up to the data rate that is supported by the equipment in the wireless network.	T=O	
WLAN-WI-23	The WIDS shall log the signal strength of hardware operating in the coverage area of the WIDS sensors.	T=O	
WLAN-WI-24	The WIDS shall detect and log when it receives 802.11 frames being sent with a transmit power above maximum transmit power levels according to country regulations.	T=O	
WLAN-WI-25	The WIDS should support user-defined and customizable attack signatures.	T=O	
WLAN-WI-26	The WIDS shall detect RF-based Denial-of-Service (DoS) attacks.	T=O	
WLAN-WI-27	The WIDS shall perform protocol anomaly analysis to detect violations of WLAN standards such as 802.11 and 802.1X.	T=O	
WLAN-WI-28	The WIDS shall detect and log deauthentication flooding.	T=O	
WLAN-WI-29	The WIDS shall detect and log disassociation flooding.	T=O	
WLAN-WI-30	The WIDS shall use anomaly-based detection, to detect, log, and generate an alert when the network's activity deviates from an established network baseline.	O	Optional
WLAN-WI-31	The WIDS shall monitor bandwidth usage.	O	Optional
WLAN-WI-32	The WIDS shall monitor number of users/wireless clients.	O	Optional
WLAN-WI-33	The WIDS shall monitor times of usage.	T=O	
WLAN-WI-34	The WIDS shall track the connection status of each client (authorized or unauthorized) in real time including, but not limited to, whether the client is offline, associated, or authentication is pending.	T=O	
WLAN-WI-35	The WIDS shall detect and log illegal state transitions, such as a client device transmitting data frames through an AP to a network device before being associated and authenticated.	T=O	
WLAN-WI-36	The WIDS shall detect and log an event where an attacker spoofs the Media Access Control (MAC) address of an authorized client to attempt to connect to the legitimate network.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-37	The WIDS shall detect and log an event where two sensors in physically separate (non-overlapping) locations (such as different buildings) receive frames with the same MAC address at the same time.	T=O	
WLAN-WI-38	The WIDS shall detect and log an event where a whitelisted EUD's MAC address appears in multiple physically distant locations.	O	Optional
WLAN-WI-39	The WIDS shall detect whitelisted EUDs establishing peer-to-peer connections with other whitelisted devices or unauthorized devices.	O	Optional
WLAN-WI-40	The WIDS shall detect EUDs bridging two network interfaces (wired and wireless). If the wired interface is connected to the internal network and the wireless interface is connected to a Rogue AP, this can expose traffic from the internal network.	O	Optional
WLAN-WI-41	The WIDS shall detect and log the presence of an 802.11 bridge.	T=O	
WLAN-WI-42	The WIDS shall detect and log the presence of a single device transmitting beacons looking for a bridge.	T=O	
WLAN-WI-43	The WIDS shall detect and log the presence of two or more devices transmitting bridge data frames.	T=O	
WLAN-WI-44	The WIDS shall provide the ability to remove or disable all WIDS components' non-secure communications paths used for management and event monitoring including HTTP, SNMPv1, File Transfer Protocol (FTP), and Telnet.	T=O	
WLAN-WI-45	The WIDS shall allow for alert notification filtering such as alert notification type, severity levels, and number of alerts to receive.	T=O	
WLAN-WI-6	The WIDS alert notifications shall be descriptive to show the significance of alerts.	T=O	
WLAN-WI-47	The WIDS must support the ability to export event logs and reports into industry standard formats such as Comma Separated Values (CSV) and Common Log Format (CLF).	T=O	

12.10 Configuration Change Detection Requirements

Table 19. Configuration Change Detection (CM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CM-1	A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	T=O	
WLAN-CM-2	An automated process shall ensure that configuration changes are logged.	T=O	
WLAN-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	T=O	
WLAN-CM-4	All Solution components shall be configured with a monitoring service that detects all changes to configuration.	T=O	

12.11 Device Management Requirements

Only authorized Security Administrators will be allowed to administer the Components. The WLAN solution will be used as transport for the Secure Shell (SSH)v2, IPsec, or TLS data from the Administration Workstation to the Component.

Table 20. Device Management (DM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-DM-1	Administration Workstations shall be dedicated for the purposes given in the CP and shall be physically separated from workstations used to manage non-CSfC solutions.	T=O	
WLAN-DM-2	All administration shall be performed through direct physical access or from an Administration Workstation remotely through SSHv2, IPsec, or TLS.	T=O	
WLAN-DM-3	Antivirus software shall be running on all Administration Workstations.	T=O	
WLAN-DM-4	All components shall be configured to restrict the IP address range for the network administration device to the smallest range possible.	T=O	
WLAN-DM-5	The Gray Management network shall not be directly connected to Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-DM-6	All administration of solution components shall be performed from an Administration Workstation remotely using one of SSHv2, IPsec, or TLS 1.2 or later version; or by managing the solution components locally.	T=O	
WLAN-DM-7	Security Administrators shall authenticate to solution components before performing administrative functions.	T	WLAN-DM-11
WLAN-DM-8	Security Administrators shall authenticate to solution components with Suite B-compliant certificates before performing administrative functions remotely.	O	WLAN-DM10
WLAN-DM-9	Security Administrators shall establish a security policy for EUDs per the implementing organization's local policy.	T=O	
WLAN-DM-10	EUDs shall generate logs and send to a central SIEM in the Red network.	O	Optional
WLAN-DM-11	Security Administrators shall initiate certificate signing requests for solution components as part of their initial keying within the solution.	T=O	
WLAN-DM-12	Devices shall use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	O	Optional
WLAN-DM-13	The WLAN Access System and solution components within the Gray network shall forward log entries to a SIEM on the Gray Management network (or SIEM in the Red Network if using an AO approved one-way tap) within 10 minutes.	T=O	
WLAN-DM-14	All logs forwarded to a SIEM on the Gray Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	T	WLAN-DM-15
WLAN-DM-15	All logs forwarded to a SIEM on a Red Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	O	WLAN-DM-14
WLAN-DM-16	When managing Solution components over the Black network, the management traffic shall be encrypted with Suite B algorithms IAW Table 9.	T=O	

12.12 Continuous Monitoring Requirements

Table 21. Continuous Monitoring (MR) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-MR-1	Traffic from the Gray or Red networks shall be monitored from an Intrusion Detection System (IDS).	T	WLAN-MR-2
WLAN-MR-2	Traffic from the Gray or Red networks shall be monitored from an Intrusion Prevention System (IPS).	O	WLAN-MR-1
WLAN-MR-3	The WIDS shall encrypt and sign all alerts pushed to a remote system administrator.	O	WLAN-MR-4
WLAN-MR-4	System administrators shall authenticate all alerts received by the WIDS.	T	WLAN-MR-3
WLAN-MR-5	All event monitoring of the WIDS shall be remotely performed from the Gray Management Network through SSHv2, IPsec, or TLS.	T=O	
WLAN-MR-6	The IDS in the solution shall be configured to send alerts to the Security Administrator.	T	WLAN-MR-7
WLAN-MR-7	The IPS in the solution shall be configured to block malicious traffic flows and alert the Security Administrator.	O	WLAN-MR-6
WLAN-MR-8	The IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	T	WLAN-MR-9
WLAN-MR-9	The IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	WLAN-MR-8
WLAN-MR-10	The IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	T	WLAN-MR-11
WLAN-MR-11	The IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	WLAN-MR-10
WLAN-MR-12	A Network-based Intrusion Detection System (NIDS) shall be deployed on the Gray Management Network to monitor traffic arriving from or leaving to the WLAN Access System.	O	Optional
WLAN-MR-13	The NIDS shall report all matches to the attack signatures on the NIDS to both inbound and outbound traffic.	O	Optional
WLAN-MR-14	The NIDS shall be regularly updated with attack signatures in accordance with local policy.	O	Optional

12.13 AUDITING REQUIREMENTS

Table 22. Auditing (AU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AU-1	VPN Gateways shall log establishment of a VPN tunnel.	T=O	
WLAN-AU-2	VPN Gateways shall log termination of a VPN tunnel.	T=O	
WLAN-AU-3	VPN Clients shall log establishment of a VPN tunnel.	T=O	
WLAN-AU-4	VPN Clients shall log termination of a VPN tunnel.	T=O	
WLAN-AU-5	Solution components shall log all actions performed on the audit log (off-loading, deletion, etc.).	T=O	
WLAN-AU-6	Solution components shall log all actions involving identification and authentication.	T=O	
WLAN-AU-7	Solution components shall log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.	T=O	
WLAN-AU-8	Solution components shall log all actions performed by a user with super-user or administrator privileges.	T=O	
WLAN-AU-9	Solution components shall log escalation of user privileges.	T=O	
WLAN-AU-10	Solution components shall log generation, loading, and revocation of certificates.	T=O	
WLAN-AU-11	Solution components shall log changes to time.	T=O	
WLAN-AU-12	Each log entry shall record the date and time of the event.	T=O	
WLAN-AU-13	Each log entry shall include the identifier of the event.	T=O	
WLAN-AU-14	Each log entry shall record the type of event.	T=O	
WLAN-AU-15	Each log entry shall record the success or failure of the event to include failure code, when available.	T=O	
WLAN-AU-16	Each log entry shall record the subject identity.	T=O	
WLAN-AU-17	Each log entry shall record the source address for network-based events.	T=O	
WLAN-AU-18	Each log entry shall record the user and, for role-based events, role identity, where applicable.	T=O	
WLAN-AU-19	Auditors shall detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AU-20	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated CRL to the Security Administrator.	O	Optional
WLAN-AU-21	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate.	O	
WLAN-AU-22	The WIDS shall log when sensors fail to communicate.	T=O	
WLAN-AU-23	The EUD shall log all successful and unsuccessful logins.	O	Optional
WLAN-AU-24	The EUD shall log all successful and unsuccessful logouts.	O	Optional
WLAN-AU-25	The EUD shall audit installation and removal of software.	O	Optional
WLAN-AU-26	The EUD shall audit attempts to change security-relevant configuration items.	O	Optional
WLAN-AU-27	The EUD shall audit changes to security-relevant configuration items.	O	Optional
WLAN-AU-28	The EUD shall audit signature verification and certificate validation.	O	Optional
WLAN-AU-29	Auditors shall compare and analyze collected network flow data against the established baseline on at least a weekly basis.	T=O	

12.14 Key Management Requirements

12.14.1 General Requirements

Table 23. PKI General (KM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-1	Certificates and user private keys shall be classified to the level determined by the AO and compliant with CNSSI 4005.	T=O	
WLAN-KM-2	A locally-operated CA supporting the VPN Gateway shall be physically separate from a locally-supported CA supporting the Wireless Controller and Authentication Server.	T = O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-3	All public/private key pairs and certificates for the VPN Gateway and Wireless Controller and Authentication Server shall be used for authentication only.	T=O	
WLAN-KM-4	The Outer and Inner CAs shall each operate in compliance with Certificate Policy and Certification Practice Statement (CPS) that are formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	T=O	
WLAN-KM-5	The Gray and Inner CAs shall rekey infrastructure devices and EUDs prior to expiration of keys.	T=O	
WLAN-KM-6	Authentication certificates issued by the Gray and Inner CAs for the Solution shall be X.509 v3 certificates as defined in ITU-T Recommendation X.509.	T=O	
WLAN-KM-7	All device certificates issued by the Gray and Inner CAs, and their corresponding private keys, shall be treated as CUI (or higher as determined by the AO).	T=O	
WLAN-KM-8	CAs shall run anti-virus software.	T=O	
WLAN-KM-9	CAs shall not escrow private keys.	T=O	
WLAN-KM-10	If multiple Red enclaves exist in the WLAN Solution and the Outer CA resides in the Red network, the Outer CA must reside in the Red network with the highest classification level.	T=O	
WLAN-KM-11	Outer CAs shall provide services through either the Gray or Red network.	T=O	
WLAN-KM-12	Inner CAs shall provide services through the Red Network.	T=O	
WLAN-KM-13	All certificates issued by the Outer and Inner CAs for the WLAN Solution shall be Non-Person Entity (NPE) certificates.	T=O	
WLAN-KM-14	Authentication certificate profiles for the Gray and Inner CAs for the WLAN Solution shall comply with IETF RFC 5280.	T=O	
WLAN-KM-15	The key sizes and algorithms for CA certificates and authentication certificates issued to Authentication Server, the VPN Gateway, and Administrative Device Components shall be as illustrated in Table 8.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-16	Private keys associated with on-line, locally run Outer and Inner CAs shall be protected using Hardware Security Modules (HSMs) validated to at least FIPS 140-2 Level 2. "On-line" means the CA is always powered on and network-accessible.	T=O	

12.14.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 24. Certificate Issuance Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-17	Gray and Red Management Services Components shall be initially keyed and loaded with certificates within a physical environment certified to protect the highest classification level of the MA solution network.	T=O	
WLAN-KM-18	Outer and Inner CAs shall use Public Key Cryptographic Standard (PKCS)#10 and PKCS#7 to issue authentication certificates to Outer WLAN Components, Inner VPN Components, and Gray and Red Management Services Components.	T	WLAN-KM-21
WLAN-KM-19	Red and Gray Management Services shall use PKCS#12 for installing certificates/keys to EUDs.	T	WLAN-KM-20
WLAN-KM-20	Red and Gray Management Services shall use PKCS#7 for installing certificates to EUDs.	O	WLAN-KM-19
WLAN-KM-21	Outer and Inner CAs shall use IETF RFC 7030 Enrollment over Secure Transport (EST) to issue authentication certificates to Outer WLAN Components, Inner VPN Components, and Gray and Red Management Services Components.	O	WLAN-KM-18
WLAN-KM-22	Certificate signing requests Gray and Red Management Services Components shall be submitted to the CA in accordance with the CA's Certificate Policy and Certification Practices Statement (CPS).	T=O	
WLAN-KM-23	Outer and Inner CAs shall issue certificates in accordance with their Certificate Policies and CPSs.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-24	Certificate Policies and CPSs for non-Enterprise, locally-run CAs shall ensure the CAs issue certificates within a defined and limited name space and assert: • Unique Distinguished Names (DNs) • Appropriate key usages • A registered policy Object Identifier (OID)	T=O	
WLAN-KM-25	Outer and Inner CAs shall assert at least one CRL Distribution Point (CDP) Uniform Resource Locater (URL) in certificates issued to Solution Infrastructure VPN Gateway, Wireless controller and Authentication Server, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRLs.	T=O	
WLAN-KM-26	The key validity period for certificates issued by non-Enterprise, locally run CAs to WLAN EUDs shall not exceed 14 months.	T=O	
WLAN-KM-27	The key validity period for certificates issued by non-Enterprise, locally run CAs to WLAN Solution Infrastructure Components shall not exceed 36 months.	T=O	
WLAN-KM-28	Inner CAs shall only issue certificates to the VPN Gateway and Red Network Components of WLAN Solutions.	T=O	
WLAN-KM-29	Outer CAs shall only issue certificates to Wireless Controller and Authentication Server.	T=O	
WLAN-KM-30	The Outer CA shall issue certificates to the WLAN Authentication Server that contains the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage extension.	O	Optional
WLAN-KM-31	The Outer CA shall issue certificates to WLAN Clients that contain the Client Authentication OID (1.3.6.1.5.5.7.3.2) in the ExtendedKeyUsage field and in the extended KeyUsage field and the Key Agreement bit is set in the Key Usage field OID (2.5.29.15.4)	T=O	
WLAN-KM-32	The VPN Gateway shall only trust the Inner CA used for its network.	T=O	
WLAN-KM-33	WLAN Components shall only trust the Outer CA used within the solution.	T=O	

12.14.3 CERTIFICATE RENEW AND REKEY REQUIREMENTS

Table 25. Certificate Renew and Rekey Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-34	Certificate renewal or rekey shall occur prior to a certificate expiring.	T=O	
WLAN-KM-35	Certificate renewal or rekey shall be performed in accordance with the CA's Certificate Policy and CPS.	T=O	
WLAN-KM-36	Outer and Inner CAs shall issue renewed/ rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7.	T	WLAN-KM-37
WLAN-KM-37	Outer and Inner CAs shall issue renewed/rekeyed authentication certificates to Solution Components using EST (RFC 7030).	O	WLAN-KM-36

12.14.4 CERTIFICATE REVOCATION REQUIREMENTS

Table 26. Certificate Revocation Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-38	Outer and Inner CAs shall revoke a certificate issued to WLAN Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	T=O	
WLAN-KM-39	Outer and Inner CAs shall make certificate revocation information available in the form of CRLs signed by the CAs.	T=O	
WLAN-KM-40	CRLs shall be X.509 v2 CRLs as defined in ITU-T Recommendation X.509.	T=O	
WLAN-KM-41	CRL profiles shall comply with IETF RFC 5280.	T=O	
WLAN-KM-42	Procedures for requesting certificate revocation shall comply with the CA's Certificate Policy and Certification Practices Statement.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-KM-43	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure revocation procedures address the following: • Response for a lost, stolen or compromised WLAN EUD • Removal of a revoked infrastructure device (i.e., VPN Gateway) from the network • Re-establishment of a WLAN Solution Component whose certificate was revoked • Revocation of certificates due to compromise of an WLAN EUD • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP addresses	T=O	
WLAN-KM-44	Outer and Inner CAs shall make CRLs available to authorized CRL Distribution Points (CDPs), so that the CRLs can be accessed by Solution Components.	T=O	
WLAN-KM-45	Enterprise CAs shall create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	T=O	
WLAN-KM-46	Non-enterprise, locally run CAs shall publish new CRLs at least once every 28 days.	T=O	
WLAN-KM-47	Non-enterprise, locally run CAs shall publish a new CRL within one hour of a certificate being revoked.	T=O	
WLAN-KM-48	Solution Infrastructure Components shall have access to new certificate revocation information within 24 hours of the CA creating a new CRL.	T=O	
WLAN-KM-49	Non-enterprise, locally run CAs shall ensure that newly created CRLs are published at least 7 days prior to the expiration of the current CRLs.	T=O	
WLAN-KM-50	The WLAN Solution shall provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Server on the Red and Gray network that is compliant with IETF RFC 6960.	O	Optional
WLAN-KM-51	Certificate revocation status messages delivered by an OCSP server shall be digitally signed and compliant with IETF RFC 6960.	O	Optional

12.15 FIREWALL REQUIREMENTS (FW)

Table 27. Gray Firewall Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-FW-1	Gray Network Firewall shall permit IKE and IPsec traffic between the EUDs VPN Client and VPN Gateway protecting networks of the same classification level.	T=O	
WLAN-FW-2	Gray Network Firewall shall allow HTTP traffic between the Authentication Server and Gray CDP or OCSP responder.	T	WLAN-FW-3 and WLAN-FW-4
WLAN-FW-3	Gray Network Firewall shall allow HTTP GET requests from the Authentication Server to the Gray CDP or OCSP responder for the URL of the CRL needed by the VPN Gateway, and block all other HTTP requests.	O	WLAN-FW-2
WLAN-FW-4	Gray Network Firewall shall allow HTTP responses from the Gray CDP or OCSP responder to the Authentication Server that contain a well-formed CRL per IETF RFC 5280, and block all other HTTP responses.	O	WLAN-FW-2
WLAN-FW-5	Gray Network Firewall shall only accept management traffic on the physical ports connected to the Gray Management network.	T=O	
WLAN-FW-6	Gray Network Firewall shall only permit packets whose source and destination IP addresses match the external interfaces of the VPN Components that support Red networks of the same classification level.	T=O	
WLAN-FW-7	Gray Network Firewall shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O	
WLAN-FW-8	Gray Network Firewall shall deny all traffic that is not explicitly allowed by requirements WLAN-FW-1, WLAN-FW-2, WLAN-FW-3, WLAN-FW-4, or WLAN-FW-5.	T=O	
WLAN-FW-9	Gray Network Firewall shall allow control plane traffic (NTP, DHCP, DNS).	T=O	

13 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

13.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS (GD)

The following requirements shall be followed regarding the use and handling of the solution.

Table 28. Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-1	All Solution Infrastructure components shall be physically protected as classified devices, classified at the highest classification level of the Red network.	T=O	
WLAN-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the solution Infrastructure components.	T=O	
WLAN-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to EUDs.	T=O	
WLAN-GD-4	All components of the solution shall be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O	
WLAN-GD-5	EUDs using a NSA-approved DAR solution shall be disposed of in accordance with the disposal requirements for the DAR solution.	T=O	
WLAN-GD-6	All EUDs shall have their certificates revoked prior to disposal.	T=O	
WLAN-GD-7	Users shall periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	T=O	
WLAN-GD-8	Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.	T=O	
WLAN-GD-9	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the CP.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-10	The AO will ensure that a compliance audit shall be conducted every year against the latest version of the WLAN CP as part annual solution re-registration process.	T=O	
WLAN-GD-11	Results of the compliance audit shall be provided to and reviewed by the AO.	T=O	
WLAN-GD-12	Customers interested in registering their solution against the WLAN CP shall register with NSA and receive approval prior to AO authorization to operate.	T=O	
WLAN-GD-13	The implementing organization shall complete and submit a WLAN CP requirements compliance matrix to their respective AO.	T=O	
WLAN-GD-14	Registration and re-registration against the WLAN CP shall include submission of WLAN CP registration forms and compliance matrix to NSA.	T=O	
WLAN-GD-15	When a new approved version of the WLAN CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months.	T=O	
WLAN-GD-16	Solution implementation information, which was provided to NSA during solution registration, shall be updated annually (in accordance with Section 15.3) as part annual solution re-registration process.	T=O	
WLAN-GD-17	Audit log data shall be maintained for a minimum of 1 year.	T=O	
WLAN-GD-18	The amount of storage remaining for audit events shall be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	T=O	
WLAN-GD-19	Audit data shall be frequently off-loaded to a backup storage medium.	T=O	
WLAN-GD-20	A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	T=O	
WLAN-GD-21	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-22	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long- term storage.	T=O	
WLAN-GD-23	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.	T=O	
WLAN-GD-24	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	T=O	
WLAN-GD-25	Strong passwords shall be used that comply with the requirements of the AO.	T=O	
WLAN-GD-26	Security critical patches shall be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	T=O	
WLAN-GD-27	Local policy shall dictate how the Security Administrator will install patches to solution components.	T=O	
WLAN-GD-28	Solution components shall comply with local TEMPEST policy.	T=O	
WLAN-GD-29	Software, settings, keys, and all other configuration data persistently stored on EUDs shall be handled as controlled unclassified information or higher classification.	T=O	
WLAN-GD-30	All hardware components shall be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution.	T=O	

Additional WLAN-GD requirements can be found in Section 14.

13.2 Requirements for Incident Reporting

Error! Reference source not found. lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators, Certificate Authority Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution,

personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary, but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Error! Reference source not found. only provides requirements directly related to the incident reporting process. See Section 12.12 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 29. Incident Reporting Requirements (RP)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-RP-1	Solution owners shall report confirmed incidents meeting the criteria in WLAN RP-3 through WLAN-RP-16 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O	
WLAN-RP-2	At a minimum, the organization shall provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Name of affected Network(s) • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	T=O	
WLAN-RP-3	Solution owners shall report a security failure in any of the CSfC solution components.	T=O	
WLAN-RP-4	Solution owners shall report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC Solution.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-RP-5	For Gray network interfaces, solution owners shall report any malicious inbound and outbound traffic.	T=O	
WLAN-RP-6	Solution owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O	
WLAN-RP-7	Solution owners shall report if a solution component sends traffic with an unauthorized destination address.	T=O	
WLAN-RP-8	Solution owners shall report any malicious configuration changes to the components.	T=O	
WLAN-RP-9	Solution owners shall report any unauthorized escalation of privileges to any of the CSfC solution components.	T=O	
WLAN-RP-10	Solution owners shall report if two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	T=O	
WLAN-RP-11	Solution owners shall report any evidence of malicious physical tampering with solution components.	T=O	
WLAN-RP-12	Solution owners shall report any evidence that one or both of the layers of the solution failed to protect the data.	T=O	
WLAN-RP-13	Solution owners shall report any significant degradation of services provided by the solution.	T=O	
WLAN-RP-14	Solution owners shall report malicious discrepancies in the number of connections established the WLAN Access System.	T=O	
WLAN-RP-15	Solution owners shall report malicious discrepancies in the number of VPN connections established by the Inner VPN Gateway.	T=O	

14 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the WLAN solution. Security Administrator duties include, but are not limited to, the following:

1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the WLAN solution.

5) Ensuring that the implemented WLAN solution remains compliant with the latest version of this CP.

6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include, but are not limited to, the following:

1) Administering the CA, including authentication of all components requesting certificates.

2) Maintaining and updating the CRL.

3) Provisioning and maintaining EUD certificates in accordance with this CP for implementations that include them.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the WLAN solution. Auditor duties include, but are not limited to, the following:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to Outer and Inner administrative components.

Solution Integrator – In certain cases, an external integrator may be hired to implement a WLAN solution based on this CP. Solution Integrator duties may include, but are not limited to, the following:

1) Acquiring the products that compose the solution.

2) Configuring the WLAN solution in accordance with this CP.

3) Documenting, testing, and maintaining the solution.

4) Responding to incidents affecting the solution.

End User –An End User may operate an EUD from physical locations not owned, operated, or controlled by the government. The End User shall be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. Remote User duties include, but are not limited to the following:

1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.

2) Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Additional policies related to the personnel that perform these roles in a WLAN Solution are as follows:

Table 30. Role-Based Personnel Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-31	The Security Administrator, CAAs, Auditor, EUD User, and Solution Integrators shall be cleared to the highest level of data protected by the Solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement.	T=O	
WLAN-GD-32	The Security Administrator, CAA, and Auditor roles shall be performed by different people.	T=O	
WLAN-GD-33	All Security Administrators, CAAs, EUD Users, and Auditors shall meet local Information Assurance (IA) training requirements.	T=O	
WLAN-GD-34	The CAA(s) for the Inner tunnel shall be different individuals from the CAA(s) for the Outer tunnel.	O	Optional
WLAN-GD-35	Upon discovering an EUD is lost, stolen or altered, an EUD User shall immediately report the incident to their Security Administrator and Certificate Authority Administrator.	T=O	
WLAN-GD-36	Upon notification of a lost, stolen or altered EUD, the Certificate Authority Administrators shall revoke that EUD's certificates.	T=O	
WLAN-GD-37	The Security Administrator(s) for the Inner Encryption Endpoints and supporting components on Enterprise/Red networks shall be different individuals from the Security Administrator(s) for the Outer VPN Gateway and supporting components on Gray networks.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-38	Administrators shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	O	Optional
WLAN-GD-39	The Auditor shall review all logs specified in this CP at least once a week.	T=O	
WLAN-GD-40	Security Administrators shall initiate the certificate revocation process prior to disposal of any solution component.	T=O	
WLAN-GD-41	Auditing of the Outer and Inner CA operations shall be performed by individuals who were not involved in the development of the Certificate Policy and CPS, or integration of the WLAN solution.	T=O	

15 INFORMATION TO SUPPORT AO

This section details items that likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the WLAN solution, see Section 15.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 15.2.
- The customer provides the results from testing and system certification and accreditation to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 15.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/IAD Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit shall be conducted every year against the latest version of the WLAN CP, and the results shall be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the Solution Components in the solution in the case of a compromise.

- The AO will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO will report incidents affecting the solution in accordance with Section 13.2.

The system AO maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO shall ensure that the solution remains properly configured with all required security updates implemented.

15.1 Solution Testing

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a WLAN solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the WLAN solution. The entire solution, to include each component described in Section 5, is addressed by this test plan including the following:

1) Set up the baseline network and configure all components.
2) Document the baseline network configuration. Include product model and serial numbers, and software version numbers at a minimum.
3) Develop a test plan for the specific implementation using the test requirements from Section 16. Any additional requirements imposed by the local AO should also be tested, and the test plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.
4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black box testing and Gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO for approval of the solution.

The following testing requirement has been developed to ensure that the WLAN solution functions properly and meets the configuration requirements from Section 12. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 31. Test Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-TR-1	The organization implementing the CP shall perform all tests listed in Section 16.	T=O	

15.2 Risk Assessment

The risk assessment of the WLAN solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

15.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where WLAN CP solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the IAD Director is published, customers will have six months to bring their solutions into compliance with the new version of the CP and re-register their solution (see requirement WLAN-GD-15). Customers are also required to update their registrations whenever the information provided on the registration form changes.

16 TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure that they have properly configured the solution. As defined in Section 10, in order to comply with this CP, a solution must at minimum implement all Threshold requirements associated with each of the

capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO regarding compliance of the solution with this CP. Note that the details of the procedures are the responsibility of the final developer of the solution test plan in accordance with AO-approved network procedures. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented.

16.1 Product Selection

This section contains procedures to verify that the components in this CP were selected to ensure independence in several important features.

Requirements being tested: WLAN-PS-1 through WLAN-PS-14

Procedure Description:

1) For the Inner VPN Gateways, perform the following:
   a) Verify that Gateways are on the list of IPsec VPN Gateways on the CSfC Components List. (WLAN-PS-1)
2) For the WLAN Access System, perform the following:
   a) Verify that the WLAN Access System is on the list of WLAN Access Systems on the CSfC Components List. (WLAN-PS-2)
3) For each EUD, perform the following:
   a) Verify the EUD is on the list of Mobile Platforms on the CSfC Components List. Note that WLAN Clients on the Mobile Platforms on the CSfC Components List are also considered as being on the CSfC Components List. (WLAN-PS-3, WLAN-PS-4)
   b) Verify the VPN Client is on the list of IPsec VPN Clients on the CSfC Components List. (WLAN-PS-5)
   c) Verify the EUD's Inner VPN Client and WLAN Client either come from different manufacturers or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. (WLAN-PS-11)
4) For the IPS, perform the following:
   a) Verify that the IPS is from the list of IPS's on the CSfC Components Lists. (WLAN-PS-6)
5) For the Gray firewall, perform the following:

a) Verify that the firewalls are on the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List. (WLAN-PS-7)

6) For the Inner VPN Gateway, the Gray Firewall, and the WLAN Access System, perform the following:

a) Verify that the Inner VPN Gateway and the WLAN Access System either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (WLAN-PS-8)

b) Verify that the Wireless Access System, Inner VPN Gateway, Gray Firewalls, and Inner Encryption Components are physically separate components such that no component is used for more than one function. (WLAN-PS-9)

c) Verify that the cryptographic libraries used by the VPN Gateway and the WLAN Access System either come from different independent manufacturers or, if from the same manufacturer, that NSA has determined that sufficient implementation independence exists. (WLAN-PS-12)

7) For the CAs, perform the following:

a) Verify the Inner and Outer CAs are either from different independent manufacturers or, if from the same manufacturer, that NSA has determined that sufficient implementation independence exists. (WLAN-PS-10)

8) For all components in the solution, perform the following:

a) Verify that each component has gone through a Product Supply Chain Threat Assessment. (WLAN-PS-13)

b) Verify that the components are configured to use the NIAP-certified evaluated configuration. (WLAN-PS-14)

Expected Result:

The results of the inspection should reveal that the WLAN Campus Solution components conform to the WLAN Campus CP.

16.2 Overall Solution

Requirements being tested: WLAN-SR-1 through WLAN-SR-6

Procedure Description:

1) Verify that all default accounts, passwords, community strings and other default access controls have been either changed or removed. (WLAN-SR-1)

2) Verify that the time of day on the VPN Gateway is synchronized with a time source located in the Red network. (WLAN-SR-2)

3) Verify that the time of day on the WLAN Authentication Server, the WLAN Controller and Gray network Firewall by logging on to check that they are synchronized with the same time source located in the Gray Management network. (WLAN-SR-3)

4) Verify that all components are properly configured in accordance with local policy and applicable U.S. Government guidance. (WLAN-SR-4)

5) Verify that virus signatures are updated on Solution Components as required by policy. (WLAN-SR-5)

6) Verify that all physical paths leaving the Red network transits through the WLAN solution in accordance with this CP or via an AO-approved solution. (WLAN-SR-6)

Expected Result:

16.3 End User Device Configurations

This section contains a procedure to ensure that the configurations for all the EUDs in the WLAN solution follow the requirements given in this CP.

Requirements being tested: WLAN-EU-1 through WLAN-EU-35, WLAN-DM-9

Procedure Description:

1) For the EUD:

   a) Ensure that only authorized administrators can change configurations by attempting to change the EUDs network configuration as a normal user. (WLAN-EU-1)

   b) Ensure that there are separate authentication and privileges for administrator and user roles by identifying the different password protections and verifying they are not shared. (WLAN-EU-2)

   c) Verify that only AO-approved software is loaded to the EUD by obtaining a list of approved software that is allowed. (WLAN-EU-3)

   d) Verify that only authorized administrators can install or remove software by attempting to install/remove as a normal user. (WLAN-EU-4)

   e) Verify that the EUD is configured to require a user login prior to granting access to any EUD functionality. (WLAN-EU-5)

f) Ensure that the EUD is configured to limit the number of incorrect login attempts per an AO-approved period of time by either erasing the configuration and data stored on the device or by prohibiting login attempts for a AO-approved period of time. (WLAN-EU-6), (WLAN-EU-30)

g) Ensure that the EUD is configured to lock the screen and require user re-authentication after an AP-approved period of inactivity by verifying the configuration file on the EUD. (WLAN-EU-13), (WLAN-EU-29)

h) Verify the configuration file of the EUD to ensure that Global Positioning Systems (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO have been disabled.(WLAN-EU-18).

i) Verify the configuration file of the EUD to ensure that all cellular access is disabled.(WLAN-EU-19)(WLAN-EU-21)

j) Verify the configuration file of the EUD to all network and wireless interfaces are disabled except for 802.11. (WLAN-EU-20)

k) Verify the configuration file for the EUD to ensure that the password for use-to-device authentication is a minimum of 4 alpha-numeric case sensitive characters. (WLAN-EU-23)

l) Verify the configuration file of the EUD to ensure a unique X.509 device certificate signed by the Outer CA is used for authentication with the Wireless Access System. (WLAN-EU-25)

m) Verify the configuration file for the EUD to ensure a unique X.509 device certificate signed by the Inner CA is used for authentication with the VPN Gateways. (WLAN-EU-26)

n) Verify the configuration that all display notifications are disabled when the device is in a locked state. (WLAN-EU-32)

o) Verify the configuration that USB mass storage mode is disabled on the EUD.(WLAN-EU-33)

p) Verify the configuration that USB data transfer capability is disabled on the EUD.(WLAN-EU-34)

2) For the EUD, verify in the policy the following:

a) Verify the local policy to ensure that rekeying of EUDs certificates associated private keys are done through re-provisioning prior to expiration of keys. (WLAN-EU-7, WLAN-EU-8)

b) Verify the local policy to ensure that EUDs are deauthorized from the network and submitted for Forensic Analysis if suspected of being compromised. (WLAN-EU-9)

c) Verify the local policy to ensure that EUDs are destroyed if it has been determined to be compromised through Forensic Analysis. (WLAN-EU-10)

d) Verify the local policy to ensure that Users can successfully authenticate themselves prior to obtaining access to Red network services using an AO-approved method. (WLAN-EU-11), (WLAN-EU-12)

e) Verify the local policy to ensure that all Users sign an organization-defined user agreement before being authorized use of an EUD. (WLAN-EU-14), (WLAN-EU-16)

f) Verify the local policy to ensure that all Users receive organization-developed training prior to operating an EUD. (WLAN-EU-15)

g) Verify the local policy to ensure that EUDs are dedicated solely for the use for the Campus WLAN solution.(WLAN-EU-17)

h) Verify the local policy to ensure that EUD certificates are revoked and resident image removed prior to disposal of the device. (WLAN-EU-22)

i) Verify the local policy to ensure that if an NSA-Approved DAR solution is not implemented on the EUD, the native DAR protection is enabled on the device. (WLAN-EU-24).

j) Verify the local policy to ensure that the maximum password lifetime is less than 181 days. (WLAN-EU-27).

k) Verify the local policy to ensure that all unnecessary keys are destroyed for the EUD secure key storage during provisioning. (WLAN-EU-30).

l) Verify the local policy to ensure that all unnecessary X.509 certificates are removed from the EUD Trust Anchor Database during provisioning.(WLAN-EU-31).

m) Verify the local policy to ensure that prior to the installation of new applications, the application digital signature is verified. (WLAN-EU-35).

Expected Result:

The results of the test should reveal that the EUD conform to the Campus WLAN CP; results are pass/fail.

16.4 WLAN CLIENT

Requirements being tested: WLAN-WC-1 and WLAN-WC-2.

Procedure Description: For the WLAN Client

1) Verify that the EUD establishes the WLAN Client tunnel at start-up. (WLAN-WC-1)

2) Verify that the WLAN AS certificate chain is rooted by the WLAN trusted root CA. (WLAN-WC-2)

This test procedure verifies that the WLAN Clients are checking the Distinguished Name and Subject Alternate Name attributes of the WLAN Authentication Server certificate during authentication.

Requirements being tested: WLAN-WC-3

Procedure Description:

1) Generate a TLS certificate that does not contain values in the Distinguished Name and Subject Alternative Name fields that appear in the whitelist used by the WLAN Clients, and load the certificate onto the WLAN Authentication Server.
2) For each EUD, perform the following:
   a) Power on the EUD.
   b) Verify that the EUD is unable to connect to the WLAN. (WLAN-WC-3)
   c) Shut down the EUD.
3) Generate a TLS certificate that does contain values in the Distinguished Name and Subject Alternative Name fields that appear in the whitelist used by the WLAN Clients, and load the certificate onto the WLAN Authentication Server.
4) For each EUD, perform the following:
   a) Power on the EUD.
   b) Verify that the EUD is able to connect to the WLAN. (WLAN-WA-7)
   c) Shut down the EUD.

Expected Result:
In Step 2(b), the EUDs should fail to connect to the WLAN. In Step 4(b), the EUDs should be able to connect to the WLAN.

This test procedure verifies that each EUD has been configured with appropriate WLAN Client certificates.
Requirements being tested: WLAN-WC-4, WLAN-WC-12
Procedure Description:

5) For EUD, perform the following:
   a) Verify that its WLAN Client has been loaded with a device certificate that has not been loaded on any other EUD or other component in the system. (WLAN-WC-4)
   b) Verify that its WLAN Client has been loaded with a CA (signing) certificate that can be used to verify the signature on the device certificate. (WLAN-WC-4)
   c) Verify that its WLAN Client's device certificate has an extendedKeyUsage field that indicates support for Client Authentication (OID 1.3.6.1.5.5.7.3.2). (WLAN-WC-12)

Expected Result: In Step 1, the device certificate used by each EUD's WLAN Client should adhere to the desired properties.

This test procedure verifies that WLAN Clients notify the EUD's user that its certificate is about to expire.

Requirements being tested: WLAN-WC-6
Procedure Description:

6) Identify the amount of advance notice users should receive before their EUD's WLAN Client certificate expires.
7) For EUD, perform the following:
    a) Generate a TLS certificate with a lifetime of five minutes plus the amount of time identified in Step 1 and load it onto the EUD's WLAN Client.
    b) Wait five minutes.
    c) Verify that the WLAN Client has alerted the user that its device certificate is due to expire. (WLAN-WC-6)

This test procedure verifies that the EUDs cannot be used to bridge the WLAN to an external network.

Requirements being tested: WLAN-WC-9
Procedure Description:
8) For EUD, perform the following:
    a) Inspect the EUD's networking configuration to verify that only one physical network interface is enabled. (WLAN-WC-9)

Expected Result:
In Step 1(a), the EUD should be unable to connect to two different networks simultaneously.

16.5 Key Management

This section contains a procedure to ensure that key management capabilities for the WLAN solution follow the requirements given in this CP.

Requirements being tested: WLAN-KM-1 through WLAN-KM-49, WLAN-AU-36 through WLAN-AU-38, WLAN-PF-3

Procedure Description:

1) Perform the following to validate the correct deployment of CAs:

a) For CAs, verify the configuration of the WLAN Solution to ensure that Outer CAs deliver services through either the Gray or Red networks; and, Inner CAs only deliver services through the Red network. (WLAN-KM-2, WLAN-KM-3)

b) For CAs, verify that the Outer and Inner CAs are physically separate from one another. (WLAN-KM-2)

c) For Locally-run CAs that operate on-line, verify the CAs utilize FIPS 140-2 Level 2 or higher Hardware Security Modules (HSMs) to protect the CAs' private signing keys. (WLAN-KM-16)

d) For all CAs, verify that the CA does not have access to any WLAN Solution Component private keys. (WLAN-KM-11)

Expected Results: CAs are correctly deployed and in compliance with requirements WLAN-KM-1 through WLAN-KM-4, WLAN-KM-11 and WLAN-KM-16.

2) Perform the following to validate the structure of certificates issued by CAs:

a) Obtain a sample set of test certificates issued to WLAN solution components.

b) Verify the Distinguished Name in each certificate identifies a Non-Person Entity (NPE), unless that certificate is used in a TLS EUD where a user certificate is required. In this case, the certificate DN identifies a human user. (WLAN-KM-13)

c) Verify the Key Usage extension in the each certificate only asserts "digitalSignature". (WLAN-KM-6)

d) Verify the certificates are compliant with the data standard for Version 3 certificates defined in ITU-T Recommendation X.509. (WLAN-KM-6)

e) Verify the certificates are compliant with IETF RFC 5280 profile requirements. (WLAN-KM-14)

f) Verify the certificates are compliant with the key sizes and algorithms specified in Tables 8-9. (WLAN-KM-15)

Expected Results: The Certificate structure and content are compliant with requirements WLAN-KM-6 and WLAN-KM-13 and WLAN-KM-15.

3) Perform the following to validate correct policy implementation as it relates to CAs and certificates issued by the CAs:

a) Verify the CA has a Certificate Policy and a Certification Practices Statement (CPS) in place that is compliant with IETF RFC 3647, and that the CA operates in accordance with the policy and CPS. (WLAN-KM-4,)

b) Verify that the WLAN Solution policy states device authentication certificates issued by the CA, along with corresponding private keys, are considered Controlled Unclassified Information (CUI), and user private keys are classified to the level determined by the AO. (WLAN-KM-1, WLAN-KM-7)

Expected Results: CA policy exists and complies with requirements WLAN-KM-7 and WLAN-KM-14.

4) Perform the following Steps to validate the certificate issuance capability of the WLAN solution:

a) Verify that a physical environment is identified to initially load keys and certificates onto WLAN Solution Components, where the environment is certified to protect information at the highest classification level of the WLAN Solution red network. (WLAN-KM-17)

b) Verify that the key and certificate provisioning process for WLAN Solution Components ensures private keys are never escrowed. (WLAN-KM-9)

c) Generate a public/private key pair for the Outer VPN Component that complies with the key size and algorithm requirements in Tables 8-9. If the Component is capable of generating its own key pair, the key pair is to be generated on the Component. Else, the key pair is generated by a dedicated management workstation.

d) Generate a certificate request for the Outer VPN Component, and ensure the request complies with PKCS#10.

e) Submit the certificate request to the Outer CA, and verify that the CA returns a signed certificate using PKCS#7. (WLAN-KM-18)

f) If the key pair was generated by a management workstation, install the certificate and private key using PKCS#12. If the key pair was generated by the VPN Component, install the signed certificate using PKCS#7. (WLAN-KM-19, WLAN-KM-20)

g) Repeat Steps 4c through 4f for each Inner Encryption Component of the WLAN Solution.

h) If the WLAN Solution supports IETF RFC 7030 (Enrollment over Secure Transport (EST)), verify that the certificate request, response and installation process complies for WLAN Solution Components complies with EST. (WLAN-KM-21)

i) Verify that the certificate request and issuance processes comply with the Outer and Inner CAs' Certificate Policies and CPSs. (WLAN-KM-22, WLAN-KM-23)

j) For locally run CAs, verify the Certificate Policies and CPSs to ensure certificate issued by the CAs: 1) enforce unique Distinguished Names (DNs); 2) assert key usages as defined by WLAN-KM-5; and 3) assert a registered policy Object Identifier (OID).

k) For locally run CAs, examine the contents of a sample set of issued certificates to ensure that the certificates assert: 1) unique Distinguished Names (DNs); 2) key usages as defined by WLAN-KM-5; and 3) a registered policy OID. (WLAN-KM-24)

l) For all CAs, examine the contents of a sample set of issued certificates and ensure that at least one valid CRL Distribution Point (CDP) is asserted in the CDP extension of the certificates. (WLAN-KM-25)

m) For locally run CAs, ensure the validity periods asserted in certificates issued by the CAs do not exceed 14 months for WLAN End User Devices (EUDs). (WLAN-KM-26)

n) For locally run CAs, ensure the validity periods asserted in certificates issued by the CAs do not exceed 36 months for WLAN Solution Infrastructure Components. (WLAN-KM-27)

o) Verify that the Inner CAs can only issue certificates to Inner Encryption Components and Red Network Components. (WLAN-KM-28)

p) Verify that the Outer CAs can only issue certificates to Outer VPN Components and Gray Network Components. (WLAN-KM-29)

Expected Results:

For Step 4a, a physical environment exists to initially load keys and certificates onto WLAN Solution Components, where the environment is certified to protect information at the highest classification level of the WLAN Solution Red network.

For Step 4b, private keys for WLAN Solution Components cannot be escrowed.

For Steps 4c-4e, the certificate request/response process between the WLAN Solution Component and the CAs correctly implements PKCS#10 and PKCS#7.

For Step 4f, the key and certificate installation process correctly implements PKCS#12 or PKCS#7.

For Step 4g, same results as for Steps 4c through 4f.

For Step 4h, the certificate request/response process between the WLAN Solution Component and the CAs correctly implements EST.

For Step 4i, the certificate request/response process complies with the CAs' Certificate Policies and CPSs.

For Step 4j-4n, the contents of certificates issued by the CAs comply with requirements WLAN-KM-24 through WLAN-KM-27.

For Step 4o, Inner CAs can only issue certificates to Inner Encryption Components and Red Network Components.

For Step 4p, Outer CAs can only issue certificates to Outer VPN Components and Gray Network Components.

For Step 4q, Enterprise Root CA shall issue certificates the Subordinate CAs for the Red and Gray networks respectively.

For Step 4r, the Subordinate CAs shall issue certificates for the inner and outer tunnels.

5) Perform the following Steps to validate the certificate renewal and rekey capability of the WLAN solution:

   a) Verify that the certificate renew and rekey processes comply with the Outer and Inner CAs' Certificate Policies and CPSs. (WLAN-KM-35)

   b) Verify that the Outer and Inner CAs' Certificate Policies and CPSs require certificate renew and rekey be performed prior to a certificate expiring. Verify the Outer and Inner CAs' Certificate Policies and CPSs require an WLAN Solution Component go through the initial certificate issuance process if the certificate is expired. (WLAN-KM-34)

   c) Generate a new public/private key pair for the Outer VPN Component that complies with the key size and algorithm requirements in Tables 8-9. If the Component is capable of generating its own key pair, the key pair is to be generated on the Component. Else, the key pair is generated by a dedicated management workstation.

   d) Generate a certificate renew and rekey request for the Outer VPN Component, and ensure the request complies with PKCS#10.

   e) Submit the certificate request to the Outer CA, and verify that the CA returns a signed certificate using PKCS#7. (WLAN-KM-32)

   f) Repeat Steps 5c through 5e for each Inner Encryption Component of the WLAN Solution.

   g) If the WLAN Solution supports IETF RFC 7030 (Enrollment over Secure Transport (EST)), verify the certificate renew and rekey request, response and installation process complies for WLAN Solution Components complies with EST. (WLAN-KM-35)

Expected Results:

For Step 5a, the certificate renewal and rekeying request/response process complies with the CAs' Certificate Policies and CPSs.

For Step 5b, the CAs' Certificate Policies and CPSs require certificate renew and rekey to be performed prior to the certificate expiring. If the certificate is expired, the Certificate Policies and CPSs require the WLAN Solution Component go through the initial certificate issuance process.

For Steps 5c-5e, the certificate renewal and rekeying request/response process between the WLAN Solution Component and the CAs correctly implements PKCS#10 and PKCS#7.

For Step 5f, the key and certificate installation process for certificate renewal and rekeying correctly implements PKCS#12 or PKCS#7.

For Step 5g, same results as for Steps 5c through 5f.

For Step 5h, the certificate renewal and rekeying request/response process between the WLAN Solution Component and the CAs correctly implements EST.

6) Perform the following Steps to validate the certificate revocation and CDP capabilities of the WLAN solution:

   a) Verify that the Outer and Inner CAs' Certificate Policies and CPSs define requirements and procedures for revoking WLAN Solution Component certificates, where certificate revocation is required when the binding between the subject information and public key within the certificate is no longer considered valid. (WLAN-KM-36)

   b) Verify that the Outer and Inner CAs' Certificate Policies and CPSs define requirements and procedures for requesting the revocation of WLAN Solution Component certificates. (WLAN-KM-40)

   c) For locally run CAs, verify the Outer and Inner CAs' Certificate Policies and CPSs define certificate revocation requirements and procedures for WLAN Solution Components that address: 1) response to a lost, stolen or compromised WLAN EUD; 2) removal of a revoked WLAN infrastructure device from the WLAN Solution network; 3) re-establishment of a WLAN Solution Component after certificate revocation is performed; 4) revocation of certificates when a WLAN EUD is considered compromised; and 5) revocation of certificates if simultaneous use of the certificate is detected from different IP addresses. (WLAN-KM-41)

d) Verify that the Outer and Inner CAs has the capability to generate CRLs after certificate revocation functions are performed. (WLAN-KM-37)

e) Obtain CRLs from the Outer and Inner CAs and ensure their structures are compliant with the data standard for Version 2 CRLs defined in ITU-T Recommendation X.509, and with the CRL profile standard defined by IETF RFC 5280. (WLAN-KM-38, WLAN-KM-39)

f) Obtain CRLs from the Outer and Inner CAs and upload them onto the CDPs defined for the WLAN Solution. Depending on the WLAN Solution configuration, Outer CA CRLs can be uploaded onto Black and/or Outer CDPs; Inner CA CRLs can be uploaded onto Gray and/or Red CDPs.

g) Verify that WLAN Solution Components can access the CDPs and download the CRLs issued by the Outer and Inner CAs via HTTP. Outer VPN Components and Gray Management Service Components are able to access and download the CRL issued by the Outer CA; Inner Encryption Components and Red Management Service Components are able to access and download the CRL issued by the Inner CA. (WLAN-KM-42, WLAN-PF-3)

h) For Enterprise CAs, verify that the Certificate Policies and CPSs define requirements and procedures for publishing CRLs. (WLAN-KM-43)

i) For locally run CAs, verify that the Certificate Policies and CPSs define requirements and procedures for 1) publishing new CRLs at least once every 28 days; 2) creating a new CRL within one hour of a certificate being revoked; and 3) publishing a newly created CRL at least 7 days before the expiration of the current CRL. (WLAN-KM-44, WLAN-KM-45, WLAN-KM-47)

j) Verify the WLAN Solution has procedures defined to transfer new CRLs to WLAN Solution CDPs within 24 hours of the CRLs being created. (WLAN-KM-46)

k) For WLAN Solutions that support the On-Line Certificate Status Protocol (OCSP) to provide certificate revocation status information, verify the OCSP Servers are deployed on the Gray and Red networks to deliver OCSP responses in accordance with IETF RFC 6960. (WLAN-KM-48)

l) Generate an OCSP request from the Outer VPN Gateway and send the request to the OCSP Server operating in the Gray network.

m) Generate an OCSP response from the OCSP Server in the Gray network and deliver it to the Outer VPN Gateway.

n) Examine the OCSP Response, and verify that it is digitally signed and compliant with IETF RFC 6960. (WLAN-KM-49)

o) Repeat Steps 6l-6n for all WLAN Solution Inner Encryption Components using an OCSP Server operating in the Red network. (WLAN-KM-49)

Expected Results:

For Steps 6a-6c, the Certificate Policies and CPSs have requirements and procedures defined to satisfy requirements WLAN-KM-36, WLAN-KM-40 and WLAN-KM-41.

For Steps 6d and 6e, the CAs are able to generate Version 2 CRLs that are compliant with ITU-T Recommendation X.509 and IETF RFC 5280.

For Steps 6f and 6g, WLAN Solution Components successfully access and download CRLs from CDPs deployed in the Gray and Red networks of the WLAN Solution.

For Steps 6h and 6i, the Certificate Policies and CPSs have requirements and procedures defined to satisfy requirements WLAN-KM-43 through WLAN-KM-45, and WLAN-KM-47.

For Step 6j, procedures exist to transfer new CRLs to WLAN Solution CDPs within 24 hours of the CRLs being created. (WLAN-KM-46)

For Steps 6k through 6o, OCSP Servers are correctly deployed in the Gray and Red networks and issue digitally signed OCSP responses compliant with IETF RFC 6960 to WLAN Solution Components. (WLAN-KM-48 and WLAN-KM-49)

16.6 Solution Filtering Configurations

This section contains a procedure to ensure that the filtering configurations for all the WLAN solution follow the requirements given in this CP.

Requirements being tested: WLAN-PF-1 through WLAN-PF-2, WLAN-PF- 4 through WLAN-PF-16

Procedure Description:

1) Perform the following Steps on the each of the Solution Components:

a) Log into the component.

b) Verify through the configuration file that network interfaces are restricted to the smallest address range, ports, and protocols (WLAN-PF-1).

c) Verify through the configuration file that all unused network interfaces are disabled (WLAN-PF-2).

2) For the Outer VPN Gateway perform the following:

    a) Obtain the current configuration for the Outer VPN Gateway.

    b) Verify that the requirements WLAN-PF-4, WLAN-PF-7 or WLAN-PF-8, , WLAN-PF-9 through WLAN-PF-12 are met.

3) For the Inner VPN Gateway perform the following:

    a) Obtain the current configuration for the Inner VPN Gateway.

    b) Verify the requirements WLAN-PF-5.

4) Establish a connection from the EUD to the Red network.

    a) Using a protocol analyzer on the Outer firewall, observe inbound and outbound traffic on the Outer firewall.

    b) Verify that the only protocols that are allowed through are IKE, ESP, and control plan protocols as specified in WLAN-PF-13.

5) For the Inner firewall perform the following:

    a) Log into the Inner firewall.

    b) Obtain the configuration file.

    c) Verify that the Inner firewall has a whitelist for all Inner Encryption Endpoints (WLAN-PF-6).

6) For the EUDs consisting of a single computing platform

    a) Verify there is no ingress or egress of Certificate Revocation traffic (OCSP queries, HTTP GET to CDPs) on the Black interface. (WLAN-PF-14)

    b) Verify there is no ingress or egress of Name Resolution traffic (e.g. DNS query/response) on the Black interface. (WLAN-PF-15)

    c) Verify there is no ingress and egress of NTP traffic on the Black interface. (WLAN-PF-16)

Expected Result:

For Step 1, the Solution components network interfaces are configured properly. For Step 2- 4, the Outer, Inner VPN Gateway, and Outer firewall are only allowing the necessary protocols. For Step 5, verify that the Inner firewall is configured correctly. For Step 6, verify there is no

Certificate Revocation, name resolution, or NTP traffic between the EUDs and the Black network.

16.7 Configuration Change Detection

This section contains a procedure to ensure that changes made to any of the WLAN Solution configurations are detected by the Configuration Change Detection tool.

Requirements being tested: WLAN-CM-1 through WLAN-CM-3

Procedure Description:

1) The following shall be performed for each of the Solution components within this CP.

   a) Log into the Solution components (Outer firewall, Outer VPN Gateway, Gray firewall, Gray Management Services, Inner Encryption Endpoints, Red Management Services, EUD, and Retransmission Device (if applicable)).

   b) Compare the current version of the Solution Component's configuration with the stored baseline and ensure the current version matches the stored configuration. (WLAN-CM-1)

   c) Make a change to the configuration, preferably something that is not fundamental to the security of the WLAN solution.

   d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from 1c are recorded. (WLAN-CM-2).

   e) Inspect the monitoring service to verify that the service has detected a change in configuration. (WLAN-CM-3)

Expected Result:

The Auditor will validate the baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change. Lastly if there was a configuration change, a monitoring service will detect a change in the configuration.

16.8 Continuous Monitoring

This section contains procedures for ensuring traffic is monitored for and alerts generated for potential unauthorized/malicious traffic. It also contains procedures for ensuring a SIEM is in place to collect logs and that it is configured correctly.

Requirements being tested: WLAN-MR-1 through WLAN-MR-18

Procedure Description:

1) Ensure that an IDS/IPS is deployed to monitor traffic in at least one of three locations (WLAN-MR-1 through WLAN-MR-6):
    a) Between the Outer firewall and Outer VPN Gateway (M1)
    b) Between the Outer VPN Gateway and the Gray firewall (M2)
    c) On the internal side of the Inner firewall (M3)
2) Ensure that each IDS/IPS in the solution is configured to send alerts to the Security Administrator, and, where possible, block malicious traffic. (WLAN-MR-7, WLAN-MR-8)
3) Ensure that each IDS/IPS in the solution is configured with rules that will generate alerts and, where possible, block traffic for any unauthorized source and destination IP addresses (WLAN-MR-9 through WLAN-MR-12).
4) Ensure that an SIEM is implemented (WLAN-MR-13 – WLAN-MR-16).
    a) Ensure the SIEM is implemented in the Gray network.
    b) Otherwise, if the SIEM is implemented within the Enterprise/Red network, ensure devices are configured to push events to an Enterprise/Red SIEM and through an AO-approved one-way tap.
    c) Send packets expected to be blocked by the Outer VPN Gateway or Gray firewall. Ensure the SIEM sends alerts to the Auditor when anomalous behavior such as this is detected.
    d) Ensure that logs from the Outer VPN Gateway Gray firewall and any other components located within the Gray Management Services are collected on the Gray SIEM.
    e) Ensure these logs are encrypted with TLS, SSHv2, or IPSEC.
5) Ensure that any one-way taps are deployed as per WLAN-MR-17 – WLAN-MR-18.
    a) Ensure that any one-way taps deployed as part of the solution are approved for use by the AO.
    b) Ensure that the SIEM implemented at the Red level that collects black and/or gray monitoring data sent through any one-way tap is deployed in an enclave isolated from the Red/Enterprise Network.
    c) Ensure that monitoring data flowing from M2 and/or M1 can transit to the SIEM if implemented at the Red level.
    d) Attempt to send other data through the one-way taps to determine if this data is blocked.

Expected Result:

For Steps 1 – 3, an IDS or IPS is in place to monitor, block where possible, and send alerts as appropriate. For Steps 4 and 5, an SIEM shall be implemented either in the Gray network or the Red/Enterprise network via one-way taps, as approved by the AO and only monitoring data will be able to transit through these taps.

16.9 AUDIT

This section contains procedures for ensuring audit events are detected, the proper information is logged for each event, and there is a procedure detailed in the CPS documentation for auditing each CA device.

Requirements being tested: WLAN-DM-14, WLAN-DM-15, WLAN-AU-1 through WLAN-AU-22, WLAN-AU-29 through WLAN-AU-35, WLAN-DM-10, WLAN-DM-16, WLAN-DM-17

Procedure Description:

1) Examples for testing the ability of each WLAN Component to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with Section 12.13.

    a) All actions performed by a user with super-user privileges (auditor, administrator, etc.) and any escalation of user privileges. (WLAN-AU-12, WLAN-AU-13)\

        i) Log in as an administrator to the Solution Infrastructure Components or a EUD.

        ii) Perform a variety of administrator actions on the Solution Infrastructure Components or EUD.

        iii) Verify that a log entry was created for each action taken in Step ii that required super-user privileges and also states the escalation of privileges.

        iv) If performing an action on anEUD, verify that the EUD is generating logs and sends the logs to the central SIEM. (WLAN-DM-10)

        v) Revert back to the baseline configuration, eliminating the changes made in Step ii.

        vi) Repeat the above with the Auditor role.

    b) Changes to time. (WLAN-AU-15)

        i) Log in as a Security Administrator to the Solution Infrastructure Components.

        ii) Modify the system time on the Solution Infrastructure Components by at least 1 hour.

iii) Verify that a log entry was created due to the change in system time and by whom.

iv) Revert the system time back to the accurate time of day.

c) Log into and out of the WLAN Solution as a normal user and send traffic to the Red Network. Then log into the central SIEM as an Auditor, and inspect the audit entry for the following: WLAN-DM-14, WLAN-DM-15.

i) Verify that the log on as a normal user is logged and has an identifiable code for the type of event. (WLAN-AU-10, WLAN-AU-18)

ii) Verify that the log entry identifies the subject accessing the solution. (WLAN-AU-20)

iii) Verify that the log entry identifies the event. (WLAN-AU-17)

iv) Verify that the log entry includes the time, date, and the time zone offset. (WLAN-AU-16)

d) Establish and terminate a VPN tunnel. Verify in the logs, that these two events were logged. (WLAN-AU-1, WLAN-AU-3, WLAN-AU-5, WLAN-AU-7)

i) Establish and terminate a TLS connection. Verify in the logs, that these two events were logged. (WLAN-AU-2, WLAN-AU-4, WLAN-AU-6, WLAN-AU-8)

e) Log into a Solution Infrastructure Components as a Security Administrator and delete previously recorded audit log. Verify the log recorded this deletion. (WLAN-AU-9)

f) As the Certificate Authority Administrator, log into the audit log and attempt to delete a log entry. Verify this action is recorded with a failure code. (WLAN-AU-11, WLAN-AU-19)

g) Verify a log entry was created for the attempted unauthorized action.

2) Verify the source address, user, and for role-based events, role identity for all audit log entries is recorded. (WLAN-AU-21, WLAN-AU-22)

3) Verify that all logs forwarded to a SIEM on a Gray Management network are configured to be encrypted while in transit using SSHv2, IPSEC, or TLS with the appropriate Suite B algorithm supported by the solution. (WLAN-DM-16)

4) Verify that all logs forwarded to a SIEM on a Red Management network are configured to be encrypted while in transit using SSHv2, IPSEC, or TLS with the appropriate Suite B algorithm supported by the solution. (WLAN-DM-17)

5) Verify that the procedure WLAN-AU-35 is currently in place by the implementing organization and are followed.

6) Verify that the Outer VPN Gateway and Inner Encryption Components log the failure to pull the CRL from the Inner or Outer CDP. (WLAN-AU-29, WLAN-AU-30)

   a) CDP Servers shall remove all CRLs.

   b) Outer VPN Gateways and Inner Encryption Components shall attempt to pull the CRL from their respective CDPs.

   c) Review the Outer VPN Gateway and Inner Encryption Components audit logs to verify that a log report is generated from failure to pull the CRL.

7) Verify that the Outer VPN Gateway and Inner Encryption Components log if the version of the CRL on the Inner or Outer CDP is older than the current cached CRL. (WLAN-AU-31, WLAN-AU-32)

   a) Load the CDPs with CRLs that are older than the current cached CRLs on the Outer VPN Gateway and Inner Encryption Components.

   b) Have the Outer VPN Gateway and Inner Encryption Components attempt to pull the CRLs.

   c) Review the Outer VPN Gateway and Inner Encryption Components audit logs to verify that a log report is generated.

8) Verify that the Outer VPN Gateway and Inner Encryption Components log if signature validation of the CRL on the Inner or Outer CDP fails. (WLAN-AU-33, WLAN-AU-34)

   a) Load the CDPs with CRLs that contain an invalid signature.

   b) Have the Outer VPN Gateway and Inner Encryption Components pull the CRLs.

   c) Review the Outer VPN Gateway and Inner Encryption Components audit logs to verify that a log report is generated due to an invalid CRL signature.

9) For all Solution components, install approved certificates, generated by the approved CA, and configure the solution so that components use the certificates for authentication.

   a) Verify an entry to the Audit log has been created due to certificate loading and generation. (WLAN-AU-14)

   b) Initiate a revocation of certificates for the Solution components.

   c) Verify that an entry in the audit log has been created due to certificate revocation. (WLAN-AU-14)

Expected Result:

For Step 1, all occurrences of auditable events given should generate an entry in the audit log. For Step 2, the source address should be the WLAN Components' loopback address. For Steps 3-4, all logs forwarded on Red Management and Gray Management networks should be encrypted with the appropriate protocols. For Step 5, the procedure is followed and is in place. For Step 6-8, there should be an audit log entry created for each requirement. For Step 9, a log should be generated for generation and revocation of certificates.

16.10 EUD With Multiple Connections

This section contains a procedure to ensure that only one IPsec is allowed for the inner layer of encryption per EUD and that no other connections are permitted.

Requirements being tested: WLAN-AU-23 through WLAN-AU-28

Procedure Description:

1) For a IPsec connection, ensure that the EUD performs the following Steps:
   a) The administrator will install the same device certificates on two EUDs.
   b) The administrator will authenticate to a Red network. At the same time, the Auditor will be reviewing the logs and detect that the same device certificate is coming from two different devices. (WLAN-AU-23)
   c) The Auditor will alert the Certificate Authority Administrator to revoke the certificates and provide an updated Certification Revocation List to the Security Administrator. (WLAN-AU-25)
   d) Once the Security Administrator receives notification from the Certificate Authority Administrator, the Security Administrator will drop both sessions. (WLAN-AU-27)
2) For TLS connection, ensure that the EUD performs the following Steps:
   a) The administrator will install the same device certificates on two EUDs.
   b) The administrator will authenticate to a Red network. At the same time, the Auditor will be reviewing the logs and detect that the same device certificate is coming from two different devices. (WLAN-AU-24)
   c) The Auditor will alert the Certificate Authority Administrator to revoke the certificates and provide an updated Certification Revocation List to the Security Administrator. (WLAN-AU-26)
   d) Once the Security Administrator receives notification from the Certificate Authority Administrator, the Security Administrator will drop both sessions. (WLAN-AU-28)

Expected Result:

The same device certificate cannot be used for two devices. All results are expected to be pass/fail.

16.11 Incident Reporting Guidance

This section ensures that procedures are followed regarding incident reporting to NSA in the event a solution owner identifies a security incident which affects the solution.

Requirements being tested: WLAN-RP-1 through WLAN-RP-16

Procedure Description:

1) Verify that the procedures given in WLAN-RP-1 through WLAN-RP-16 were/are followed and are currently in place.

Expected Results:

For Step 1, all of these procedures have been followed or are in place.

16.12 Implementation of Guidance

This section ensures that there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the WLAN solution. It also ensures the personnel are in place to manage and administer this solution following the guidelines given in the CP.

Requirements being tested: WLAN-GD-1 through WLAN-GD-41, WLAN-SR-6

Procedure Description:

1) Verify the procedures for obtaining virus signature updates as required by local agency policy and the AO were/are followed and/or are in place. (WLAN-SR-9)

2) Verify the procedures given in WLAN-GD-1 through WLAN-GD-8, and WLAN-GD-17 through WLAN-GD-30 were/are followed and/or are currently in place.

3) Verify that the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (WLAN-GD-9)

4) Verify that the AO are aware that a compliance audit will be conducted every year. (WLAN-GD-10)

5) Verify that the AO is aware that they shall receive the results of the compliance audit and are responsible for reviewing the completed audit. (WLAN-GD-11)

6) Verify that the customer is aware that when they are interested in registering their solution against this CP that NSA must grant them an approval prior to the AO authorizing the solution for operation. (WLAN-GD-12)

7) Verify that the customer completes and submit the compliance matrix to their AO. (WLAN-GD-13)

8) Verify that the customer is aware that registration and re-registration against this CP includes a submission of this CP registration forms and compliance matrix to NSA. (WLAN-GD-14)

9) Verify that the customer is aware that when a new WLAN CP is published by the NSA, the AO will comply against this new CP within 6 months. (WLAN-GD-15)

10) Verify that the solution owner and AO are aware that they shall provide updated solution information to NSA on a yearly basis. (WLAN-GD-16)

11) Verify that the personnel requirements given in WLAN-GD-31 through WLAN-GD-41 are met by the personnel supporting this implementation of the WLAN solution.

Expected Result:

For Steps 1-10, all of these procedures have been followed or are in place.

16.13 Solution Functionality

This section contains a procedure for ensuring the implementing organization complies with the testing requirements.

Requirements being tested: WLAN-TR-1

Procedure Description:

1) The implementing organization's AO will inspect the test report in order to ensure all testing requirements have been met. (WLAN-TR-1)

Expected Result:

The report will ensure that the implementing organization complies with the WLAN Solution.

APPENDIX A. GLOSSARY OF TERMS

Authorization (To Operate) – The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Authorization Boundary – All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Authorizing Official – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing Official Designated Representative – An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

Authorization Package – A security package of documents consisting of the security control assessment that provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

Assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit Log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective actions are required.

Availability – Ensuring timely and reliable access to and use of information. (NIST SP 800-37).

Black Box Testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

Black Network – A network that contains classified data that has been encrypted twice. (See Section 4.1.3)

CP – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. CP instantiations are built using products selected from the CSfC Components List.

Certificate Authority (CA) – An authority trusted by one or more users to create and assign certificates. (ISO9594-8)

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (IETF RFC 3647)

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure, and confidence that only the appropriate set of individuals or organizations would be provided the information.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

CRL Distribution Point (CDP) – A web server that hosts a copy of a CRL issued by a CA for VPN Components to download (see Section 8).

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

Data Plane Protocol – A protocol that carries the data being transferred through the solution.

End User Device (EUD) – A form-factor agnostic component of the Mobile Access solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple comments to

provide physical separation between layers of encryption (see Section 4.2.1 for explanation of detailed differences between VPN EUD and TLS EUD solution design options).

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box Testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e. knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Gray Network – A network that contains classified data that has been encrypted once (see Section 4.1.2).

Gray Firewall – A stateful traffic filtering firewall placed on the Gray network to provide filtering of ports, protocols, and IP addresses to ensure traffic reaches the correct Inner Encryption Endpoint or is dropped.

Internal Interface – The interface on a VPN Gateway or Inner Encryption Component that connects to the inner network (i.e., the Gray network on the Outer VPN Gateway or the Red network on the Inner Encryption Component).

Locally Managed Device – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

Malicious – Any unauthorized events that are either unexplained or in any way indicate adversary activity.

Management Plane Protocol – A protocol that carries either traffic between a system administrator and a component being managed, or log messages from a solution component to a SIEM or similar repository.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Remotely Managed Device – A device that is being managed by any other method besides that given in the definition of a Locally Managed Device.

Security Level – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.

Split-tunneling – Allows network traffic to egress through a path other then the established VPN tunnel (either on the same interface or another network interface). Split tunneling is explicitly prohibited in WLAN CP compliant configurations (see WLAN-VT-4 and WLAN-VC-3).

SRTP Client – A component on the EUD that facilitates encryption for voice communications.

TLS Client – A component on a TLS EUD that can provides the Inner layer of DIT encryption.

TLS Component – Refers to both TLS Clients and TLS-Protected Servers.

VPN Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – A VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in a secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B. ACRONYMS

Acronym	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AO	Authorizing Official
AP	Access Point
ARP	Address Resolution Protocol
AS	Authentication Server
BIOS	Basic Input/Output System
CA	Certificate Authority
CAA	Certificate Authority Administrator
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CSV	Comma Separated Value
CUI	Controlled Unclassified Information
DAR	Data-At-Rest
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DM	Device Management
DN	Domain Name
DNS	Domain Name System
DoD	Department of Defense
DoE	Department of Energy
DoS	Denial of Service
DSA	Digital Signature Algorithm
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload

Acronym	Definition
EST	Enrollment Over Secure Transport
EUD	End User Device
FIPS	Federal Information Processing Standards
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
HIDS	Host Based Intrusion Detection System
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alert
ICT	Information Communication Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
JIMS	Joint Incident Management System
KM	Key Management
KMI	Key Management Infrastructure
MAC	Media Access Control
MDM	Mobile Device Manager
MOA	Memorandum of Agreement
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NPE	Non Person Entity
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPSEC	Operational Security
OS	Operating System
OSI	Open System Interconnection

Acronym	Definition
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMK	Pairwise-Master Key
POC	Point of Contact
PTP	Precision Time Protocol
GCM	Galois Counter Mode
RADIUS	Remote Authentication Dial in User Service
RDP	Remote Desktop Protocol
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SA	Security Association
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SIPRNet	Secret Internet Protocol Router Network
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSHv2	Secure Shell Version 2
T	Threshold
T&E	Test and Evaluation
TFFW	Traffic Filtering Firewall
TLS	Transport Layer Security
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WPA	Wi-F- Protected Access
WPA2	Wi-Fi Protected Access II

APPENDIX C. REFERENCES

CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	October 2009
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2010
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	March 2010
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*. http://www.niap-ccevs.org/pp	January 2012
NSA Suite B	*NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3))*. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006

RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013

SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	January 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al.	April 2011